S00P0302US00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

CERTIFIED COPY OF PRIORITY DOCUMENT

出 願 年 月 日
Date of Application: １９９９年 ３月１５日

出 願 番 号
Application Number: 平成１１年特許願第０６９１５２号

出 願 人
Applicant (s): ソニー株式会社

２０００年 １月２１日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特平１１－３０９５１４０

【書類名】　特許願

【整理番号】　9900143603

【提出日】　平成11年 3月15日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大石　丈於

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　岡上　拓己

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ処理装置、データ処理システムおよびその方法

【特許請求の範囲】

【請求項１】

所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、

前記暗号化したデータを記憶する記憶手段と、

同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す制御手段と

を有するデータ処理装置。

【請求項２】

前記制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項１に記載のデータ処理装置。

【請求項３】

前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する

請求項１に記載のデータ処理装置。

【請求項４】

前記制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する

請求項３に記載のデータ処理装置。

【請求項５】

前記制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項４に記載のデータ処理装置。

【請求項６】

前記制御手段は、前記処理ブロック単位で読み出した前記データを前記処理手段に出力する

請求項１に記載のデータ処理装置。

【請求項７】

前記データは圧縮されており、

前記処理手段は、前記記憶手段から読み出された前記データを、前記処理ブロックを単位として伸長する

請求項６に記載のデータ処理装置。

【請求項８】

記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムにおいて、

前記記憶装置は、

前記データ処理装置との間で相互認証処理を行う第１の相互認証処理手段と、

前記データを記憶する記憶手段と、

前記相互認証処理によって前記データ処理装置が正当な相手であると認めたときに、前記データ処理装置と前記記憶手段との間でデータの入出力を行わせる第１の制御手段と

を有し、

前記データ処理装置は、

前記記憶装置との間で相互認証処理を行う第２の相互認証処理手段と、

所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、

前記相互認証処理によって前記記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理のうち少なくとも一方を行う、前記書き込み処理において、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記憶手段に書き込み、前記読み出し処理において、前記処理ブロックを単位として前記データを前記記憶手段から読み出す第２の制御手段と

を有する

データ処理システム。

【請求項９】

前記第２の制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項８に記載のデータ処理システム。

【請求項１０】

前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する

請求項８に記載のデータ処理システム。

【請求項１１】

前記第２の制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する

請求項１０に記載のデータ処理システム。

【請求項１２】

前記第２の制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項１１に記載のデータ処理システム。

【請求項１３】

所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、

前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、

同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す

データ処理方法。

【請求項１４】

前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する

請求項１３に記載のデータ処理方法。

【請求項１５】

前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化して前記暗号化を行う

請求項１３に記載のデータ処理方法。

【請求項１６】

単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶

手段に記憶された前記暗号化されたデータを管理する

請求項１５に記載のデータ処理方法。

【請求項１７】

前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する

請求項１６に記載のデータ処理方法。

【請求項１８】

前記記憶手段から読み出された前記データを、前記処理ブロックを単位として伸長する

請求項１３に記載のデータ処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶手段に記憶するデータ処理装置、データ処理システムおよびその方法に関する。

【０００２】

【従来の技術】

例えば、著作権侵害となる不正利用を防止するために、オーディオデータなどのデータを、所定のデータ長の暗号化ブロックを単位として暗号化して記憶媒体に記憶することがある。

この場合に、暗号化しようとするデータは、通常、所定の圧縮処理ブロックを単位として圧縮されていることが多い。

【０００３】

【発明が解決しようとする課題】

ところで、上述したように圧縮されたデータを暗号化して記録媒体に記録する場合に、圧縮ブロックと暗号化ブロックとは通常一致しない。

そのため、例えば、圧縮ブロックを単位として記録媒体からデータを読み出すと、暗号化ブロックのうち一部のデータが読み出されないことがあり、正確な復号を行えなくなる。このような事態を回避するため、圧縮ブロックおよび暗号ブロックの双方を考慮して読み出しを行うと、処理が煩雑になるとう問題がある。

【０００４】

また、記録媒体に記録したデータを編集する場合などは、例えば圧縮ブロックを単位としてデータの分割および結合などが行われるが、この場合にも、編集後のデータに暗号化ブロックの一部のデータが含まれなくなる可能性が高く、同様に、正確な復号が行えなくなるという問題がある。

また、圧縮されていないデータであっても、例えば、音楽用のＣＤ(Compact Disk)フォーマットなどのように、所定のブロックを単位として処理が行われる場合にも上述した場合と同様の問題が生じる。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理フロックに基づいた処理と復号処理とを簡単な構成で正確に行うことができるデータ処理装置、データ処理システムおよびその方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第１の観点のデータ処理装置は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、前記暗号化したデータを記憶する記憶手段と、同じ前記暗号化ブロック内に位置するデー

タが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す制御手段とを有する。

【０００７】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、前記処理ブロックにデータ長調整用のデータを入れて、前記処理ブロックのデータ長が前記暗号化ブロックのデータ長の整数倍になるように調整する。

【０００８】

また、本発明のデータ処理装置は、好ましくは、前記暗号化手段は、前記暗号化を行おうとする前記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化する。

【０００９】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、単数または複数の前記処理ブロックと、当該単数または複数の処理ブロックのうち最初に暗号化された前記処理ブロック内で最初に暗号化された前記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、前記記憶手段に記憶された前記暗号化されたデータを管理する。

【００１０】

また、本発明のデータ処理装置は、好ましくは、前記制御手段は、前記単数または複数の処理ブロックを暗号化された順で前記記憶手段の連続したアドレスに記憶し、さらに、前記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順に前記記憶手段の連続したアドレスに記憶し、前記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された前記記憶手段のアドレスの直前のアドレスに前記初期値を記憶する。

【００１１】

また、本発明のデータ処理システムは、記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムであって、前記記憶装置は、前記データ処理装置との間で相互認証処理を行う第１の相互認証処理

手段と、前記データを記憶する記憶手段と、前記相互認証処理によって前記データ処理装置が正当な相手であると認めたときに、前記データ処理装置と前記記憶手段との間でデータの入出力を行わせる第１の制御手段とを有する。また、前記データ処理装置は、前記記憶装置との間で相互認証処理を行う第２の相互認証処理手段と、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、前記相互認証処理によって前記記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理のうち少なくとも一方を行う、前記書き込み処理において、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを前記憶手段に書き込み、前記読み出し処理において、前記処理ブロックを単位として前記データを前記記憶手段から読み出す第２の制御手段とを有する。

【００１２】

さらに、本発明のデータ処理方法は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、前記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、同じ前記暗号化ブロック内に位置するデータが同じ前記処理ブロック内に位置するように前記暗号化したデータを記憶手段に書き込み、前記処理ブロックを単位として前記データを前記記憶手段から読み出す。

【００１３】

【発明の実施の形態】

以下、本発明の実施形態に係わるオーディオシステムについて説明する。

図１は本実施形態のオーディオシステム１のシステム構成図、図２は図１に示す携帯用記憶装置３および携帯用プレーヤ４の内部構成図である。

図１に示すように、オーディオシステム１は、例えば、コンピュータ２、携帯用記憶装置３、携帯用プレーヤ４、ＣＤ－ＲＯＭドライブ６およびＣＤプレーヤ７を有する。

【００１４】

コンピュータ２

コンピュータ２は、ネットワーク５に接続されており、例えば、ＥＭＤ(Electronic Music Distribution: 電子音楽配信）などのサービスを提供する図示しないサービスプロバイダのホストコンピュータから、ネットワーク５を介してオーディオデータ（トラックデータ）を受信し、当該受信したオーディオデータを必要に応じて復号して、携帯用プレーヤ４に出力する。

また、コンピュータ２は、コンテンツデータを受信するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。

また、コンピュータ２は、例えば、ＣＤ－ＲＯＭドライブ６から入力したオーディオデータを携帯用プレーヤ４に出力する。

【００１５】

携帯用記憶装置３

携帯用記憶装置３は、例えば、メモリスティックであり、フラッシュメモリなどの書き換え可能な半導体メモリを内蔵している。

図２に示すように、携帯用記憶装置３は、例えば、主制御モジュール３１、通信インタフェース３２、制御モジュール３３、フラッシュメモリ３４およびフラッシュメモリ管理モジュール３５を有する。

【００１６】

〔制御モジュール３３〕

図２に示すように、制御モジュール３３は、例えば、乱数発生ユニット５０、記憶ユニット５１、鍵生成／演算ユニット５２、相互認証ユニット５３、暗号化／復号ユニット５４および制御ユニット５５を有する。

制御モジュール３３は、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール３３は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。

乱数発生ユニット５０は、乱数発生指示を受けると、６４ビット（８バイト）

の乱数を発生する。

【００１７】

記憶ユニット５１は、例えば、ＥＥＰＲＯＭ(Electrically Erasable Programmable Read Only Memory) などの不揮発性メモリであり、認証処理に必要な鍵データなどの種々のデータを記憶している。

図３は、記憶ユニット５１に記憶されているデータを説明するための図である。

図３に示すように、記憶ユニット５１は、認証鍵データIK_0～IK_{31}、装置識別データID_mおよび記憶用鍵データSK_mを記憶している。

認証鍵データIK_0～IK_{31}は、携帯用記憶装置３が携帯用プレーヤ４との間で相互認証を行う際に用いられる鍵データであり、後述するように相互認証を行う度に認証鍵データIK_0～IK_{31}のうち一の認証鍵データがランダムに選択される。なお、認証鍵データIK_0～IK_{31}および記憶用鍵データSK_mは、携帯用記憶装置３の外部から読めないようになっている。

装置識別データID_mは、携帯用記憶装置３に対してユニークに付けられた識別データであり、後述するように、携帯用記憶装置３が携帯用プレーヤ４との間で相互認証を行う際に読み出されて携帯用プレーヤ４に出力される。

記憶用鍵データSK_mは、後述するように、トラック鍵データＴＲＫを暗号化してフラッシュメモリ３４に記憶する際に用いられる。

【００１８】

鍵生成／演算ユニット５２は、例えば、ＩＳＯ／ＩＥＣ９７９７のＭＡＣ(Message Authentication Code) 演算などの種々の演算を行って鍵データを生成する。このとき、ＭＡＣ演算には、例えば、"Block cipher Algorithm"としてＦＩＰＳＰＵＢ４６－２に規定されるＤＥＳ(Data Encryption Standard)が用いられる。

ＭＡＣ演算は、任意の長さのデータを固定の長さに圧縮する一方向性ハッシュ関数演算であり、関数値が秘密鍵に依存して定まる。

【００１９】

相互認証ユニット５３は、携帯用プレーヤ４からオーディオデータを入力して

フラッシュメモリ３４に書き込む動作を行うのに先立って、携帯用プレーヤ４との間で相互認証処理を行う。

また、相互認証ユニット５３は、フラッシュメモリ３４からオーディオデータを読み出して携帯用プレーヤ４に出力する動作を行うのに先立って、携帯用プレーヤ４との間で相互認証処理を行う。

また、相互認証ユニット５３は、相互認証処理において、前述したＭＡＣ演算を行う。

当該相互認証処理では、記憶ユニット５１に記憶されているデータが用いられる。

【００２０】

暗号化／復号ユニット５４は、ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹなどのブロック暗号アルゴリズムでの暗号化を行う。使用するモードは、ＦＩＰＳ　ＰＵＢ８１”ＤＥＳ　ＭＯＤＥＳ　ＯＦ　ＯＰＥＲＡＴＩＯＮ”に規定されているようなＥＣＢ(Electronic Code Book)モードおよびＣＢＣ(Cipher Block Chaining) モードである。

また、暗号化／復号ユニット５４は、ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹなどのブロック復号アルゴリズムでの復号を行う。使用するモードは、上記ＥＣＢモードおよびＣＢＣモードである。、

当該ＥＣＢモードおよびＣＢＣモードのブロック暗号化／復号では、指定された鍵データを用いて指定されたデータを暗号化／復号する。

制御ユニット５５は、乱数発生ユニット５０、記憶ユニット５１、鍵生成／演算ユニット５２、相互認証ユニット５３および暗号化／復号ユニット５４の処理を統括して制御する。

【００２１】

〔フラッシュメモリ３４〕

フラッシュメモリ３４は、例えば、３２Ｍバイトの記憶容量を有する。

フラッシュメモリ３４には、相互認証ユニット５３による相互認証処理によって正当な相手であると認められたときに、携帯用プレーヤ４から入力したオーディオデータが書き込まれる。

また、フラッシュメモリ３４からは、相互認証ユニット５３による相互認証処理によって正当な相手であると認められたときに、オーディオデータが読み出されて携帯用プレーヤ４に出力される。

以下、フラッシュメモリ３４に記憶されるデータおよびそのフォーマットについて説明する。

図４は、フラッシュメモリ３４に記憶されるデータを説明するための図である。

図４に示すように、フラッシュメモリ３４には、例えば、トラック管理ファイル１００、トラックデータファイル101_0，101_1，101_2，101_3が記憶されている。

ここで、トラック管理ファイル１００はトラックデータファイル101_0～101_3を管理する管理データを有し、トラックデータファイル101_0～101_3はそれぞれ対応するトラックデータ（オーディオデータ）を有している。

なお、本実施形態では、トラックデータは、例えば、１曲分のオーディオデータを意味する。

【００２２】

図５は、トラック管理ファイル１００のフォーマットを説明するための図である。

図５に示すように、トラック管理ファイル１００は、トラックデータ（楽曲）毎の管理情報を記述した管理データＴＲＫＩＮＦ（０），ＴＲＫＩＮＦ（１），ＴＲＫＩＮＦ（２），ＴＲＫＩＮＦ（３）と、トラックデータ毎のパーツ情報を記述した管理データＰＲＴＩＮＦ（０），ＰＲＴＩＮＦ（１），ＰＲＴＩＮＦ（２），ＰＲＴＩＮＦ（３）とを有している。

ここで、管理データＴＲＫＩＮＦ（０）およびＰＲＴＩＮＦ（０）は、図４に示すトラックデータファイル101_0の管理データである。

管理データＴＲＫＩＮＦ（１）およびＰＲＴＩＮＦ（１）は、図４に示すトラックデータファイル101_1の管理データである。

管理データＴＲＫＩＮＦ（２）およびＰＲＴＩＮＦ（２）は、図４に示すトラックデータファイル101_2の管理データである。

管理データＴＲＫＩＮＦ（３）およびＰＲＴＩＮＦ（３）は、図４に示すトラックデータファイル101_3の管理データである。

【００２３】

ここで、ｎを０≦ｎ≦３の整数とした場合に、管理データＴＲＫＩＮＦ（ｎ）は、図６に示すように、ＦＮＭ、ＴＲＫ、Ｓ－ＳＡＭＳＥＲＩＡＬ、ＣＯＮＮＵＭ、Ｐ、ＰＮＭ１（ＯＰ）を有している。

【００２４】

ここで、ＦＮＭは、トラックデータファイル100_nの名前を示している。

ＴＲＫは、暗号化されたトラック鍵データＴＲＫを示している。

Ｓ－ＳＡＭＳＥＲＩＡＬは、図２に示す制御モジュール４３のシリアル番号を示している。

また、ＣＯＮＮＵＭは、同一のＳ－ＳＡＭＳＥＲＩＡＬ番号内で重複しないように、トラックデータファイル毎にユニークに付けられたトラック累積番号を示している。

Ｐは、トラックデータを構成するパーツ数を示している。なお、本実施形態では、パーツとは、録音開始から停止までの連続した時間内で記録されたデータの単位を示しており、通常、１トラックデータは１パーツで構成される。但し、後述するように、結合編集処理が行われると、１トラックデータに複数のパーツが含まれる場合がある。

ＰＮＭ１（ＯＰ）は、曲名ファイルへのポインタを示している。

【００２５】

また、管理データＰＲＴＩＮＦ（ｎ）は、圧縮モードなどの属性、パーツサイズなどの情報を示しており、図６に示すように、パーツ毎にＰＲＴＳＩＺＥおよびＰＫを有している。

図６に示す例では、管理データＰＲＴＩＮＦ（ｎ）が管理するトラックデータ内に、（ｍ＋１）個のパーツが含まれる場合を例示している。

ここで、ＰＲＴＳＩＺＥ（０）～（ｍ）は、それぞれ対応するパーツのクラスタサイズ、当該パーツの始まりとなるサウンドユニットＳＵおよびパーツの終わりとなるサウンドユニットＳＵを特定する情報を示している。

ＰＫ（０）～（ｍ）は、それぞれ対応するパーツのオーディオデータを暗号化するのに用いるクラスタ鍵データＣＫを生成する際に、トラック鍵データＴＲＫと共に用いられるパーツ鍵データＰＫを示している。パーツ鍵データＰＫは、パーツ毎に生成される。

【００２６】

以下、トラックデータファイル101_0～101_3について説明する。

図７は、トラックデータファイル101_0の構成を説明するための図である。

図７に示すように、トラックデータファイル101_0は、１個のパーツからなり、当該パーツが５個のクラスタＣＬ（０），ＣＬ（１），ＣＬ（２），ＣＬ（３），ＣＬ（４）で構成されている。当該パーツは、クラスタＣＬ（０）の先頭から開始し、クラスタＣＬ（４）のサウンドユニットＳＵ（４）で終了している。

なお、トラックデータファイル101_1～101_3は、基本的に、図７に示す構成をしているが、パーツ数、クラスタ数およびクラスタ内に含まれるサウンドユニットＳＵの数は、図７に示すものには限定されず、独立して決められている。

【００２７】

図８は、クラスタＣＬの構成を説明するための図である。

図８に示すように、クラスタＣＬは、連続したアドレスに順次に記憶された８バイトのブロック暗号化初期値ＩＶ、例えば、各々１６０バイトのサウンドユニットＳＵ（０）～（１０１）およびクラスタシードデータＣＳを有する。

すなわち、ブロック暗号化初期値ＩＶが、サウンドユニットＳＵ（０）の直前のアドレスに記憶されている。

ここで、ブロック暗号化初期値ＩＶは、後述するように、図２に示す暗号化／復号ユニット６４におけるＣＢＣモードの暗号化および復号に用いられる。

【００２８】

また、サウンドユニットＳＵ（０）～（１０１）は、図２に示す暗号化／復号ユニット６４においてＣＢＣ(Cipher Block Chainning)モードで６４ビット（８バイト）の暗号化ブロックを単位として暗号化して生成された８バイトの暗号文

C_i によって構成される。

本実施形態では、サウンドユニットＳＵのバイト数（例えば１６０バイト）を、暗号化の単位である暗号化ブロックのバイト数（例えば８バイト）の整数倍にしている。

すなわち、１サウンドユニットＳＵは例えば２０個の暗号文C_i からなる。

このとき、個々の暗号文C_i は一のサウンドユニットＳＵ内に位置し、一の暗号文C_i が複数のサウンドユニットＳＵに跨がって位置することはない。

ここで、フラッシュメモリ３４に記憶されているオーディオデータは、後述するように例えば、ＡＴＲＡＣ３方式で圧縮されており、当該圧縮の単位がサウンドユニットＳＵである。従って、携帯用記憶装置３から携帯用プレーヤ４にオーディオデータを読み出す場合には、読み出しの最小単位は当該サウンドユニットＳＵとなる。

このようにすることで、フラッシュメモリ３４に記憶されている暗号化されたオーディオデータにアクセスする際に、暗号化ブロックの区切りを意識する必要がなくなり、当該アクセスに伴う処理負担を軽減できる。

なお、各クラスタ内に含まれるサウンドユニットＳＵの数は、１個以上１０２個以下の範囲で任意である。

また、オーディオデータの圧縮方式は、ＡＴＲＡＣ３などのＡＴＲＡＣ方式以外のＣＯＤＥＣ方式でもよい。

クラスタシードデータＣＳは、各クラスタ毎に例えば乱数を発生して生成されたデータであり、後述するように、携帯用プレーヤ４内でクラスタ毎にクラスタ鍵データＣＫを生成する際に用いられる。

当該クラスタシードデータＣＳは、エラー対策としてクラスタ内の２箇所に格納されている。

【００２９】

〔フラッシュメモリ管理モジュール３５〕

フラッシュメモリ管理モジュール３５は、フラッシュメモリ３４へのデータの書き込み、フラッシュメモリ３４からのデータの読み出しなどの制御を行う。

【００３０】

携帯用プレーヤ４

図２に示すように、携帯用プレーヤ４は、例えば、主制御モジュール４１、通信インタフェース４２、制御モジュール４３、編集モジュール４４、圧縮／伸長モジュール４５、スピーカ４６、Ｄ／Ａ変換器４７およびＡ／Ｄ変換器４８を有する。

【００３１】

〔主制御モジュール４１〕

主制御モジュール４１は、携帯用プレーヤ４の処理を統括的に制御する。

〔制御モジュール４３〕

図２に示すように、制御モジュール４３は、例えば、乱数発生ユニット６０、、記憶ユニット６１、鍵生成／鍵演算ユニット６２、相互認証ユニット６３、暗号化／復号ユニット６４および制御ユニット６５を有する。

制御モジュール４３は、制御モジュール３３と同様に、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール４３は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。

乱数発生ユニット６０は、乱数発生指示を受けると、６４ビット（８バイト）の乱数を発生する。

記憶ユニット６１は、認証処理に必要な種々のデータを記憶している。

図９は、記憶ユニット６１に記憶されているデータを説明するための図である。

図９に示すように、記憶ユニット６１は、マスター鍵データMK_0～MK_{31}および装置識別データID_dを記憶している。

ここで、マスター鍵データMK_0～MK_{31}と、認証鍵データIK_0～IK_{31}との間には、前述した携帯用記憶装置３の装置識別データID_mを用いて、下記式（１）に示す関係がある。

なお、下記式において、ｆ（ａ，ｂ）は、例えば、引数ａ，ｂから値を導出す

る関数である。

【００３２】

【数１】

$IK_j = f(MK_j, ID_m)$ …（１）

但し、ｉは、０≦ｊ≦３１の整数。

【００３３】

また、記憶ユニット６１における認証鍵データIK_0～IK_{31}の記憶アドレスは、例えば５ビットで表現され、それぞれ記憶ユニット５１におけるマスター鍵データMK_0～MK_{31}と同じ記憶アドレスが割り当てられている。

【００３４】

鍵生成／鍵演算ユニット６２は、例えば、ＩＳＯ／ＩＥＣ９７９７のＭＡＣ演算方式を用いた演算などの種々の演算を行って鍵データを生成する。このとき、"Block cipher Algorithm"としてＦＩＰＳ　ＰＵＢ　４６－２に規定されるＤＥＳが用いられる。

【００３５】

相互認証ユニット６３は、例えば、コンピュータ２から入力したオーディオデータを携帯用記憶装置３に出力する動作を行うのに先立って、携帯用記憶装置３との間で相互認証処理を行う。

また、相互認証ユニット６３は、携帯用記憶装置３からオーディオデータを入力する動作を行うのに先立って、携帯用記憶装置３との間で相互認証処理を行う。

また、相互認証ユニット６３は、相互認証処理において、前述したＭＡＣ演算を行う。

当該相互認証処理では、記憶ユニット６１に記憶されているデータが用いられる。

なお、相互認証ユニット６３は、必要に応じて、例えば、コンピュータ２あるいはネットワーク５上のコンピュータとの間でオーディオデータの入出力を行う動作に先立って、コンピュータ２あるいはネットワーク５上のコンピュータとの間で相互認証処理を行う。

【００３６】

暗号化／復号ユニット６４は、前述したように、ＦＩＰＳ　ＰＵＢ　８１に規定されたＥＣＢモードおよびＣＢＣモードを選択的に用いてブロック暗号化を行う。

ここで、暗号化／復号ユニット６４は、ＣＢＣモードにおいて、５６ビットの鍵データｋを用いて、コンピュータ２あるいはＣＤプレーヤ７から入力したオーディオデータ（平文）を、６４ビットからなる暗号化ブロックを単位として下記式（２）に基づいて暗号化して暗号化されたオーディオデータ（暗号文）を生成する。

下記式（２）から分かるように、ＣＢＣモードでは、一つ前の暗号文と次の平文との排他的論理和を暗号化するため、同一の平文が入力されても異なる暗号文が出力され、解読が困難であるという利点がある。

【００３７】

【数２】

$$C_i = E_k\ (P_i\ \mathrm{XOR}\ C_{i-1}) \qquad \cdots (2)$$

ｉ：１以上の整数

P_i：平文（６４ビット）

C_i：暗号文（６４ビット）

ＸＯＲ：排他的論理和

E_k：５６ビットの鍵データｋを用いたＤＥＳ方式の暗号処理

【００３８】

上記式（２）の演算は、図１０で表現される。なお、図１０において、「ＩＶ」は、ブロック暗号化初期値（６４ビット）であり、図２に示す携帯用記憶装置３のフラッシュメモリ３４において、図８に示すようにクラスタＣＬ内のサウンドユニットＳＵ（０）の直前に記憶される。

【００３９】

なお、コンピュータ２あるいはＣＤプレーヤ７から入力したオーディオデータ（平文）は、ＡＴＲＡＣ(Adaptive TRansform Audio Coder)方式を改良したＡＴＲＡＣ３方式で圧縮されている。

なお、ＡＴＲＡＣは、ＭＤ(Mini Disk：商標）のための符号化圧縮方式であり、例えば、２８８ｋｂｉｔ／ｓで４４．１ｋＨｚサンプルのステレオ信号が、帯域分割とＭＤＣＴ(Modified Discrete Cosine Transform)とを併用して符号されている。すなわち、先ず、帯域分割フィルタで１／４，１／４，１／２の３つの帯域に分割され、それぞれの帯域の信号がダウンサンプルされ、時間領域の信号としてＭＤＣＴで周波数領域に変換され、当該ＭＤＣＴの係数が適応ビット配分を行ってスカラ量子化されている。

【００４０】

暗号化／復号ユニット６４は、ＦＩＰＳ８１のモードのうち、前述したＥＣＢモードおよびＣＢＣモードの復号を選択的に行う。

ここで、暗号化／復号ユニット６４は、ＣＢＣモードにおいて、５６ビットの鍵データｋを用いて、暗号文を、６４ビットからなる暗号化ブロックを単位として下記式（３）に基づいて復号して平文を生成する。

【００４１】

【数３】

$$P_i = C_{i-1} \ \mathrm{XOR} \ D_k (C_i) \qquad \cdots (3)$$

ｉ：１以上の整数

P_i：平文（６４ビット）

C_i：暗号文（６４ビット）

ＸＯＲ：排他的論理和

D_k：５６ビットの鍵データｋを用いたＤＥＳ方式の復号処理

【００４２】

上記式（３）の演算は、図１１で表現される。なお、図１１において、「ＩＶ」は、ブロック暗号化初期値（６４ビット）であり、図２に示す携帯用記憶装置３のフラッシュメモリ３４において図８に示すようにクラスタＣＬ内のサウンドユニットＳＵ（０）の直前に記憶されたものが用いられる。

【００４３】

制御ユニット６５は、乱数発生ユニット６０、記憶ユニット６１、鍵生成／鍵演算ユニット６２、相互認証ユニット６３および暗号化／復号ユニット６４の処

理を統括的に制御する。

【００４４】

〔編集モジュール４４〕

編集モジュール４４は、例えば、図４に示すように携帯用記憶装置３のフラッシュメモリ３４内に記憶されたトラックデータファイル101_0～101_3を、ユーザからの操作指示に基づいて編集して新たなトラックデータファイルを生成する。

当該編集には、１個のトラックデータファイルを分割して２個のトラックデータファイルを生成する分割編集処理と、２個のトラックデータファイルを結合して１個のトラックデータファイルを生成する結合編集処理とがある。

なお、当該編集にあたって、図５および図６に示すトラック管理ファイル１００およびトラックデータファイル101_0～101_3が書き換えられる。

編集モジュール４４における編集処理については後に詳細に説明する。

【００４５】

〔圧縮／伸長モジュール４５〕

圧縮／伸長モジュール４５は、例えば、携帯用記憶装置３から入力した暗号化されたオーディオデータを復号した後に再生する際に、ＡＴＲＡＣ３方式で圧縮されているオーディオデータを伸長し、当該伸長したオーディオデータをＤ／Ａ変換器４７に出力する。

また、例えば、ＣＤプレーヤ７あるいはコンピュータ２からから入力したオーを、携帯用記憶装置３に記憶する際に、当該オーディオデータをＡＴＲＡＣ３方式で圧縮する。

【００４６】

〔Ｄ／Ａ変換器４７〕

Ｄ／Ａ変換器４７は、圧縮／伸長モジュール４５から入力したデジタル形式のオーディオデータをアナログ形式のオーディオデータに変換してスピーカ４６に出力する。

〔スピーカ４６〕

スピーカ４６は、Ｄ／Ａ変換器４７から入力したオーディオデータに応じた音

響を出力する。

〔Ａ／Ｄ変換器４８〕

Ａ／Ｄ変換器４８は、例えば、ＣＤプレーヤ７から入力したアナログ形式のオーディオデータをデジタル形式に変換して圧縮／伸長モジュール４５に出力する。

【００４７】

以下、図１に示すオーディオシステム１の動作について説明する。

携帯用記憶装置３への書き込み動作

図１２は、携帯用プレーヤ４から携帯用記憶装置３への書き込み動作を説明するためのフローチャートである。

ステップＳ１：携帯用プレーヤ４から携帯用記憶装置３に、書き込み要求信号が出力される。

ステップＳ２：携帯用記憶装置３と携帯用プレーヤ４との間で、相互認証処理を行う際に用いる認証鍵データ$ＩＫ_{j}$の選択処理が行われる。当該処理については後述する。

ステップＳ３：携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理が行われる。当該処理については後述する。

ステップＳ４：ステップＳ３の相互認証処理によって携帯用記憶装置３および携帯用プレーヤ４の双方が相手を正当であると認めた場合には、ステップＳ５の処理が行われ、そうでない場合には処理が終了する。

ステップＳ５：携帯用記憶装置３および携帯用プレーヤ４において、セッション鍵データＳｅｋが生成される。当該処理については後述する。

ステップＳ６：携帯用プレーヤ４から携帯用記憶装置３に、通信インタフェース３２，４２を介して、暗号化したオーディオデータを出力して書き込む。当該処理については後述する。

このように、オーディオシステム１によれば、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、携帯用プレーヤ４から携帯用記憶装置３に、暗号化されたオーディオデータを書き込まれる。

そのため、著作権侵害を招くようなオーディオデータの不正な複製が容易に行われることを回避できる。

【００４８】

〔認証鍵データＩＫ$_j$ の選択処理（図１２に示すステップＳ２）〕

図１３は、認証鍵データＩＫ$_j$ の選択処理を説明するための図である。

図１３に示すように、図２に示す携帯用プレーヤ４の乱数発生ユニット６０によって６４ビットの乱数Ｒ$_j$ が生成される。

当該乱数Ｒ$_j$ は、携帯用プレーヤ４から携帯用記憶装置３に出力される。

そして、携帯用記憶装置３の相互認証ユニット５３によって、６４ビットの乱数Ｒ$_j$ の下位５ビットを用いて、記憶ユニット５１に記憶されている認証鍵データＩＫ$_0$ ～ＩＫ$_{31}$のうち一の認証鍵データＩＫ$_j$ （ｊは０≦ｊ≦３１を満たす整数）が特定される。

また、携帯用記憶装置３の記憶ユニット５１から読み出された装置識別データＩＤ$_m$ が、携帯用記憶装置３から携帯用プレーヤ４に出力される。

そして、携帯用プレーヤ４の相互認証ユニット６３によって、乱数Ｒ$_j$ の下位５ビットを用いて、マスター鍵データＭＫ$_0$ ～ＭＫ$_{31}$のうち一のマスター鍵データＭＫ$_j$ が特定される。

そして、鍵生成／鍵演算ユニット６２において、前記特定されたマスター鍵データＭＫ$_j$ と、携帯用記憶装置３から入力した装置識別データＩＤ$_m$ とを用いて、下記式（４）に基づいて、認証鍵データＩＫ$_j$ を生成する。

下記式（４）において、ｆ（ａ，ｂ）は、例えば、引数ａ，ｂから値を導出する任意の関数である。

【００４９】

【数４】

$$IK_j = f(MK_j, ID_m) \qquad \cdots (4)$$

【００５０】

これにより、携帯用記憶装置３と携帯用プレーヤ４とが、上記式（４）に示す関係を持つ認証鍵データＩＫ$_0$ ～ＩＫ$_{31}$およびマスター鍵データＭＫ$_0$ ～ＭＫ$_{31}$を有している場合には、図１３に示す処理によって同じ認証鍵データＩＫ$_j$ が選

択される。

当該選択された認証鍵データＩＫ$_j$は、後述する相互認証処理を行う際に、秘密鍵として用いられる。

また、このとき、３２個の認証鍵データＩＫ$_j$のうち選択される認証鍵データは、図１３に示す処理を行う毎に乱数Ｒ$_j$に応じてランダムに決定される。

そのため、不正な認証が成功する確率を、一の認証鍵データを固定して用いる場合の１／３２倍にすることができ、不正な認証が行われることを高い確率で回避できる。

なお、上述した実施形態では、乱数を用いて８個の認証鍵データＩＫ$_j$のうち一の認証鍵データを選択する場合を例示したが、携帯用記憶装置３および携帯用プレーヤ４の外部から入力した鍵指定信号に基づいて選択する認証鍵データを決定してもよい。

【００５１】

〔携帯用記憶装置３と携帯用プレーヤ４との間の相互認証処理（図１２に示すステップＳ３）〕

図１４は、携帯用記憶装置３と携帯用プレーヤ４との間の相互認証処理を説明するための図である。

なお、当該相互認証処理を開始するときには、前述した図１３に示す認証鍵データＩＫ$_j$の選択処理が終了しており、携帯用プレーヤ４の相互認証ユニット５３は、選択した認証鍵データＩＫ$_j$を有している。また、携帯用記憶装置３の相互認証ユニット６３は、選択した認証鍵データＩＫ$_j$、携帯用記憶装置３の装置識別データＩＤ$_m$を有している。

【００５２】

ステップＳ１０：携帯用記憶装置３の乱数発生ユニット５０において、６４ビットの乱数Ｒ$_{ms}$を生成し、これを携帯用プレーヤ４に出力する。

ステップＳ１１：携帯用プレーヤ４の乱数発生ユニット６０において、６４ビットの乱数Ｒ$_d$およびＳ$_d$を生成する。

ステップＳ１２：携帯用プレーヤ４の相互認証ユニット６３において、図１２に示すステップＳ２で得た認証鍵データＩＫ$_j$および「Ｒ$_d$ ‖ Ｒ$_{ms}$ ‖ ＩＤ$_m$」を

用いて、下記式（５）に基づいてＭＡＣ演算を行い、MAC_A を求める。

ここで、Ａ‖Ｂは、ＡとＢの連結（ｎビットのＡの後ろにｍビットのＢを結合して（ｎ＋ｍ）ビットとしたもの）を示す。

【００５３】

【数５】

$$MAC_A = MAC(IK_j, R_d \| R_{ms} \| ID_m) \quad \cdots (5)$$

【００５４】

ステップＳ１３：携帯用プレーヤ４は、「$R_d \| S_d \| MAC_A \| j$」を携帯用記憶装置３に出力する。

【００５５】

ステップＳ１４：携帯用記憶装置３の相互認証ユニット５３において、図１２に示すステップＳ２で得た認証鍵データIK_jおよび「$R_d \| R_{ms} \| ID_m$」を用いて、下記式（６）に基づいてＭＡＣ演算を行い、MAC_B を求める。

【００５６】

【数６】

$$MAC_B = MAC(IK_j, R_d \| R_{ms} \| ID_m) \quad \cdots (6)$$

【００５７】

ステップＳ１５：携帯用記憶装置３の相互認証ユニット５３において、ステップＳ１４で求めたMAC_BとステップＳ１３で入力したMAC_Aとを比較し、一致していれば、携帯用プレーヤ４が適切な認証鍵データIK_jを有していることが分かるため、携帯用記憶装置３は携帯用プレーヤ４が正当な相手であると認証する。

【００５８】

ステップＳ１６：携帯用記憶装置３の相互認証ユニット５３において、図１２に示すステップＳ２で得た認証鍵データIK_jおよび「$R_{ms} \| R_d$」を用いて、下記式（７）に基づいてＭＡＣ演算を行い、MAC_C を求める。

【００５９】

【数７】

$$MAC_C = MAC(IK_j, R_{ms} \| R_d) \quad \cdots (7)$$

【００６０】

ステップＳ１７：携帯用記憶装置３の乱数発生ユニット５０において、６４ビットの乱数S_{ms}を生成する。

【００６１】

ステップ１８：携帯用記憶装置３から携帯用プレーヤ４に、「$S_{ms} \| MAC_C$」を出力する。

【００６２】

ステップＳ１９：携帯用プレーヤ４の相互認証ユニット６３において下記式（８）に基づいてＭＡＣ演算を行い、MAC_dを求める。

【００６３】

【数８】

$$MAC_d = MAC(IK_j, R_{ms} \| R_d) \quad \cdots (8)$$

【００６４】

ステップＳ２０：携帯用プレーヤ４の相互認証ユニット６３において、ステップＳ１９で求めたMAC_dとステップＳ１８で入力したMAC_Cとを比較し、一致していれば、携帯用記憶装置３が適切な認証鍵データIK_jを有していることが分かるため、携帯用プレーヤ４は携帯用記憶装置３が正当な相手であると認証する。

以上により、携帯用記憶装置３と携帯用プレーヤ４との間の相互認証が行われる。

【００６５】

〔セッション鍵データＳｅｋの生成処理（図１２に示すステップＳ５）〕

図１５は、セッション鍵データＳｅｋの生成処理を説明するための図である。

なお、当該セッション鍵データＳｅｋの生成処理を開始するときには、前述した図１３に示す認証鍵データIK_jの選択処理および図１４に示す相互認証処理が終了しており、携帯用記憶装置３および携帯用プレーヤ４の双方は、選択した認証鍵データIK_jおよび乱数S_d，S_{ms}を有している。

【００６６】

ステップＳ３０：携帯用プレーヤ４の相互認証ユニット６３は、選択した認証

鍵データIK_jおよび「$S_d \| S_{ms}$」を用いて、下記式（９）に基づいてＭＡＣ演算を行い、セッション鍵データＳｅｋを生成する。

【００６７】

【数９】

セッション鍵データＳｅｋ＝ＭＡＣ（IK_j，$S_d \| S_{ms}$）　　…（９）

【００６８】

ステップＳ３１：携帯用記憶装置３の相互認証ユニット５３は、選択した認証鍵データIK_jおよび「$S_d \| S_{ms}$」を用いて、下記式（１０）に基づいてＭＡＣ演算を行い、セッション鍵データＳｅｋを生成する。

当該セッション鍵データＳｅｋは、正当な相手同士であれば、携帯用プレーヤ４で生成したセッション鍵データＳｅｋと同じになる。

【００６９】

【数１０】

セッション鍵データＳｅｋ＝ＭＡＣ（IK_j，$S_d \| S_{ms}$）　　…（１０）

【００７０】

〔携帯用記憶装置３へのオーディオデータの書き込み処理（図１２に示すステップＳ６）〕

図１６は、携帯用プレーヤ４から携帯用記憶装置３へのオーディオデータの書き込み処理を説明するための図である。

なお、当該書き込み処理を開始するときには、前述した図１５に示すセッション鍵データＳｅｋの生成処理は終了しており、携帯用記憶装置３および携帯用プレーヤ４は同じセッション鍵データＳｅｋを有している。

【００７１】

ステップＳ４０：携帯用プレーヤ４は、乱数発生ユニット６０にトラックデータファイル毎に乱数を発生させ、当該乱数に応じたトラック鍵データＴＲＫを生成する。

【００７２】

ステップＳ４１：携帯用プレーヤ４は、暗号化／復号ユニット６４において、ステップＳ４０で生成したトラック鍵データＴＲＫを、セッション鍵データＳｅ

ｋを用いて暗号化する。

【００７３】

ステップ４２：携帯用プレーヤ４は、ステップＳ４１で暗号化したトラック鍵データＴＲＫを携帯用記憶装置３に出力する。

【００７４】

ステップＳ４３：携帯用記憶装置３は、ステップＳ４２で入力した暗号化されたトラック鍵データＴＲＫを、暗号化／復号ユニット５４において復号する。

【００７５】

ステップＳ４４：携帯用記憶装置３は、暗号化／復号ユニット５４において、ステップＳ４３で復号したトラック鍵データＴＲＫを、記憶ユニット５１から読み出した記憶用鍵データSK_mを用いて暗号化する。

携帯用記憶装置３は、当該暗号化したトラック鍵データＴＲＫを、フラッシュメモリ３４に記憶されているトラック管理ファイル１００内の当該トラックデータに対応するＴＲＫＩＮＦ（ｎ）内に設定する。

【００７６】

ステップＳ４５：携帯用プレーヤ４は、乱数発生ユニット６０にパーツ毎に乱数を発生させ、当該乱数に応じたパーツ鍵データＰＫを生成する。また、携帯用プレーヤ４は、当該生成したパーツ鍵データＰＫを、携帯用記憶装置３のフラッシュメモリ３４に記憶されている図５および図６に示すトラック管理ファイル１００のうち対応するトラックデータファイルの管理データＰＲＴＩＮＦ（Ｎ）内に設定する。

【００７７】

ステップＳ４６：携帯用プレーヤ４は、例えば、パーツ毎に、鍵生成／演算ユニット６２において、下記式（１１）に示すように、ステップＳ４５で生成したパーツ鍵データＰＫとトラック鍵データＴＲＫとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データＴＭＫとする。

なお、テンポラリ鍵データＴＭＫの生成は、排他的論理和を用いるものには限定されず、例えば、パーツ鍵データＰＫとトラック鍵データＴＲＫとを加算する加算演算やその他の関数演算を用いるようにしてもよい。

【００７８】

【数１１】

ＴＭＫ＝ＰＫ　ＸＯＲ　ＴＲＫ　　…（１１）

【００７９】

ステップＳ４７：携帯用プレーヤ４は、乱数発生ユニット６０にクラスタ毎に乱数を発生させ、当該乱数に応じたクラスタシードデータＣＳを生成する。また、携帯用プレーヤ４は、当該生成したクラスタシードデータＣＳを、携帯用記憶装置３のフラッシュメモリ３４に記憶されている当該クラスタ内の図８に示す対応する位置に設定する。

【００８０】

ステップＳ４８：携帯用プレーヤ４は、例えば、鍵生成／鍵演算ユニット６２において、下記式（１２）に示すように、ステップＳ４６で生成したテンポラリ鍵データＴＭＫと、ステップＳ４７で生成したクラスタシードデータＣＳとを用いてＭＡＣ演算を行い、クラスタ毎にクラスタ鍵データＣＫを生成する。

【００８１】

【数１２】

ＣＫ＝ＭＡＣ（ＴＭＫ，ＣＳ）　　…（１２）

【００８２】

なお、ＭＡＣ演算の他に、例えば、ＳＨＡ－１(Secure Hash Algorithm)、ＲＩＰＥＭＤ－１６０などの一方向性ハッシュ関数(one-way hash function)の入力に秘密鍵を用いた演算を行ってクラスタ鍵データＣＫを生成してもよい。

ここで、一方向性関数ｆとは、ｘよりｙ＝ｆ（ｘ）を計算することは容易であるが、逆にｙよりｘを求めることが難しい関数をいう。

なお、一方向性ハッシュ関数については、例えば、"Handbook of Applied Cryptography,CRC Press"などに詳しく記述されている。

【００８３】

ステップＳ４９：携帯用プレーヤ４は、コンピュータ２あるいは携帯用プレーヤ４から入力したオーディオデータを、圧縮／伸長モジュール４５において、ＡＴＲＡＣ３方式で圧縮する。そして、暗号化／復号ユニット６４において、ステ

ップＳ４８で生成したクラスタ鍵データＣＫを用いて、前記圧縮したオーディオデータをＣＢＣモードで暗号化する。

【００８４】

ステップＳ５０：携帯用プレーヤ４は、ステップＳ４９で暗号化したオーディオデータを、通信インタフェース３２，４２を介して、携帯用記憶装置３に出力する。

【００８５】

ステップＳ５１：携帯用記憶装置３は、ステップＳ５０で入力した暗号化されたオーディオデータを、フラッシュメモリ３４にそのまま書き込む。

以上により、携帯用プレーヤ４から携帯用プレーヤ４へのオーディオデータの書き込み処理が終了する。

【００８６】

携帯用記憶装置３からの読み出し動作

図１７は、携帯用記憶装置３から携帯用プレーヤ４への読み出し動作を説明するためのフローチャートである。

ステップＳ６１：携帯用プレーヤ４から携帯用記憶装置３に、読み出しを要求するトラックデータ（曲）を特定した読み出し要求信号が出力される。

ステップＳ２：図１３を用いた前述したように、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理を行う際に用いる認証鍵データIK_jの選択処理が行われる。

ステップＳ３：図１４を用いて前述したように、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理が行われる。

ステップＳ４：ステップＳ３の相互認証処理によって携帯用記憶装置３および携帯用プレーヤ４の双方が相手を正当であると認めた場合には、ステップＳ５の処理が行われ、そうでない場合には処理が終了する。

ステップＳ５：携帯用記憶装置３および携帯用プレーヤ４において、セッション鍵データＳｅｋが生成される。

ステップＳ６３：暗号化されたオーディオデータを、通信インタフェース３２，４２を介して、携帯用記憶装置３から携帯用プレーヤ４に読み出す。当該処理

については後述する。

すなわち、オーディオシステム１では、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、後述するように、携帯用プレーヤ４において、携帯用記憶装置３から携帯用プレーヤ４に出力された暗号化されたトラック鍵データＴＲＫを適切なセッション鍵データＳｅｋで解読できる。

そのため、著作権侵害を招くようなオーディオデータの不正な利用が容易に行われることを回避できる。

【００８７】

〔携帯用記憶装置３からのオーディオデータの読み出し処理（図１７に示すステップＳ６３）〕

図１８は、携帯用記憶装置３から携帯用プレーヤ４へのオーディオデータの読み出し処理を説明するための図である。

なお、当該読み出し処理は、前述した図１２に示す書き込み処理の後に行われるため、図４に示すトラックデータファイル101_0～101_3には、図６に示すように、各トラックデータファイルの管理データＴＲＩＮＦ（ｎ）にトラック鍵データＴＲＫが設定され、パーツ毎にパーツ鍵データＰＫが設定され、図８に示すように各クラスタＣＬ内にはクラスタシードデータＣＳが設定されている。

また、ステップＳ５の処理が終了しているため、携帯用記憶装置３および携帯用プレーヤ４は、正当な相手同士であれば、同じセッション鍵データＳｅｋを有している。

【００８８】

ステップＳ７１：携帯用記憶装置３の暗号化／復号ユニット５４は、図４に示すようにフラッシュメモリ３４に記憶されている図５に示すトラック管理ファイル１００内のＴＲＫＩＮＦ（ｎ）のうち、読み出し要求信号で特定されるトラックデータファイルに対応するＴＲＫＩＮＦ（ｎ）内のトラック鍵データＴＲＫを、記憶ユニット５１に記憶されている記憶用鍵データSK_mを用いて復号する。

【００８９】

ステップＳ７２：携帯用記憶装置３の暗号化／復号ユニット５４は、ステップ

Ｓ７１で復号したトラック鍵データＴＲＫを、図１７に示すステップＳ５で得られたセッション鍵データＳｅｋを用いて暗号化する。

【００９０】

ステップＳ７３：携帯用記憶装置３は、ステップＳ７２で暗号化したトラック鍵データＴＲＫを携帯用プレーヤ４に出力する。

【００９１】

ステップＳ７４：携帯用プレーヤ４の暗号化／復号ユニット６４は、ステップＳ７３で携帯用記憶装置３から入力したトラック鍵データＴＲＫを、セッション鍵データＳｅｋを用いて復号する。

【００９２】

ステップＳ７５：携帯用プレーヤ４の鍵生成／演算ユニット６２は、ステップＳ７４で復号されたトラック鍵データＴＲＫと、携帯用記憶装置３のフラッシュメモリ３４に記憶されているトラック管理ファイル１００内の当該トラックデータファイルに対応するＰＲＴＩＮＦ（ｎ）に含まれるパーツ鍵データＰＫとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データＴＭＫとする。

【００９３】

【数１３】

$$TMK = PK \ \mathrm{XOR} \ TRK \qquad \cdots (13)$$

【００９４】

ステップＳ７６：携帯用プレーヤ４の鍵生成／鍵演算ユニット６２において、ステップＳ７５で生成したテンポラリ鍵データＴＭＫと、携帯用記憶装置３のフラッシュメモリ３４に記憶されている当該トラックデータファイルに対応するトラックデータファイル101_0～101_3のクラスタ内の図８に示すクラスタシードデータＣＳとを用いて、下記式（１４）に示すＭＡＣ演算を行い、当該演算結果をクラスタ鍵データＣＫとする。

クラスタ鍵データＣＫは、クラスタ毎に求められる。

【００９５】

【数１４】

$$CK = MAC(TMK, CS) \qquad \cdots (14)$$

【００９６】

ステップＳ７７：携帯用記憶装置３は、フラッシュメモリ３４に記憶されている図４に示すトラックデータファイル101_0～10_3のうち読み出し要求信号で特定されるトラックデータファイルに対応するトラックデータファイルを特定し、当該特定したトラックデータファイルを構成するクラスタ内のオーディオデータを、図８に示すサウンドユニットＳＵを単位として読み出して携帯用プレーヤ４に出力する。

【００９７】

ステップＳ７８：携帯用プレーヤ４は、暗号化／復号ユニット６４において、ステップＳ７６で生成したクラスタ鍵データＣＫを用いて、ステップＳ７７で入力したオーディオデータを復号する。

このとき、オーディオデータの復号は、各クラスタ毎に、それぞれ個別に求められたクラスタ鍵データＣＫを用いて行われる。また、復号は、暗号化の単位である８バイトのブロックを単位として行われる。

【００９８】

ステップＳ７９：携帯用プレーヤ４は、圧縮／伸長モジュール４５において、ステップＳ７８で復号したオーディオデータをＡＴＲＡＣ３方式で伸長し、当該伸長したオーディオデータを、Ｄ／Ａ変換器４７でデジタル形式に変換した後に、スピーカ４６に出力する。

このとき、圧縮／伸長モジュール４５は、ステップＳ７８で復号したオーディオデータを、サウンドユニットＳＵを単位として伸長する。

【００９９】

以上により、携帯用記憶装置３から携帯用プレーヤ４４へのオーディオデータの読み出しおよび再生が終了する。

【０１００】

〔トラックデータファイルの分割編集処理〕

前述したように、携帯用プレーヤ４の編集モジュール４４は、１個のトラックデータファイルを分割して２個のトラックデータファイルを生成する分割編集処理と、２個のトラックデータファイルを結合して１個のトラックデータファイル

を生成する結合編集処理とを行う。

先ず、分割編集処理について説明する。

図１９は、携帯用プレーヤ４の編集モジュール４４によるトラックデータファイルの分割編集処理を説明するための図である。

編集モジュール４４は、例えば、図１９（Ａ）に示す１個のトラックデータファイル（１）を、図１９（Ｂ）に示すトラックデータファイル（１）と、図１９（Ｃ）に示すトラックデータファイル（２）とに分割する。

このとき、分割の区切りとなる最小単位はサウンドユニットＳＵであり、当該例では、図１９（Ｂ）に示すように、トラックデータファイル（１）のクラスタＣＬ（２）のサウンドユニットＳＵ（３）とＳＵ（４）との間で分割されている。

【０１０１】

当該分割により、分割後のトラックデータファイル（１）のクラスタＣＬ（２）は図２０（Ａ）に示すようになり、新たに生成されたトラックデータファイル（２）のクラスタＣＬ（０）は図２０（Ｂ）に示すようになる。

このとき、図２０（Ｂ）に示すように、トラックデータファイル（２）のクラスタＣＬ（０）のサウンドユニットＳＵ（０）は分割前のトラックデータファイル（１）のクラスタ（２）のサウンドユニットＳＵ（４）となり、ラックデータファイル（２）のクラスタＣＬ（０）のサウンドユニットＳＵ（１）は分割前のトラックデータファイル（１）のクラスタ（２）のサウンドユニットＳＵ（５）となる。

また、図２０（Ｂ）に示すトラックデータファイル（２）のクラスタＣＬ（０）のブロック暗号化初期値ＩＶには、図１９（Ａ），（Ｂ）に示すトラックデータファイル（１）のクラスタＣＬ（２）内のサウンドユニットＳＵ（３）の最後の８バイトが設定される。

本実施形態では、前述したように各クラスタ内において、最初のサウンドユニットＳＵ（０）の直前にブロック暗号化初期値ＩＶを配置したことで、分割の際に、分割位置の直前の８バイトをそのままブロック暗号化初期値ＩＶとして用いれば良く、新たなトラックデータファイルを作成する際の処理を簡単にできる。

また、再生時に、サウンドユニットＳＵ（０）と共に、その直前のブロック暗号化初期値ＩＶを読み出せばよいため、再生処理も簡単になる。

【０１０２】

本実施形態では、分割前のトラックデータファイル（１）のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれＴＲＫ＿１、ＰＫ＿１およびＣＫ＿１である。

また、分割後のトラックデータファイル（１）のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれＴＲＫ＿１’、ＰＫ＿１’およびＣＫ＿１である。

また、トラックデータファイル（２）のトラック鍵データ、パーツ鍵データおよびクラスタ鍵データは、それぞれＴＲＫ＿２、ＰＫ＿２およびＣＫ＿１である。

【０１０３】

図２１は、携帯用プレーヤ４の編集モジュール４４において、新たなトラックデータファイル（２）のトラック鍵データおよびパーツ鍵データを生成する方法を説明するための図である。

分割により生成された新たなトラックデータファイル（２）は、トラックデータファイル（１）とは別に新たなトラック鍵データＴＲＫ＿２を有する。本実施形態では、パーツ鍵データＰＫ＿２を以下に示すように算出することで、クラスタ鍵データＣＫ＿１を分割前と同じにする。

【０１０４】

ステップＳ９０：編集モジュール４４は、トラックデータファイルの分割指示を入力したか否かを判断し、入力したと判断した場合にはステップＳ９１の処理を実行し、入力していないと判断した場合にはステップＳ９０の処理を繰り返す。

【０１０５】

ステップＳ９１：編集モジュール４４は、乱数発生ユニット６０に乱数を発生させ、当該乱数に応じたトラック鍵データＴＲＫ＿２を新たに生成する。

【０１０６】

ステップＳ９２：編集モジュール４４は、トラックデータファイル（２）のパーツ鍵データＰＫ＿２を下記式（１５）に基づいて生成する。

【０１０７】

【数１５】

$$PK\_2 = TRK\_1 \ \mathrm{XOR} \ PK\_1 \ \mathrm{XOR} \ TRK\_2 \quad \cdots (15)$$

【０１０８】

これにより、トラックデータファイル（２）について、前記式（１１）に基づいてされるテンポラリ鍵データは、トラックデータファイル（１）のテンポラリ鍵データと同じになり、前記式（１２）に基づいて生成されるクラスタ鍵データも分割前のクラスタ鍵データＣＫ＿１と同じにできる。

そのため、トラックデータファイル（２）内のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【０１０９】

ステップＳ９３：携帯用記憶装置３の暗号化／復号ユニット５４において、ステップＳ９１で生成したトラック鍵データＴＲＫ＿２を、記憶ユニット５１に記憶されている記憶用鍵データSK_mを用いて暗号化し、当該暗号化したトラック鍵データＴＲＫ＿２を、フラッシュメモリ３４に記憶されているトラック管理ファイル１００内の当該トラックデータファイルに対応する図６に示すＴＲＫＩＮＦに書き込む。

【０１１０】

ステップＳ９４：編集モジュール４４は、ステップＳ９２で生成したパーツ鍵データＰＫ＿２を、フラッシュメモリ３４に記憶されているトラック管理ファイル１００内の当該トラックデータファイルに対応する図６に示すＰＲＴＩＮＦにそのまま書き込む。

【０１１１】

このように、オーディオシステム１では、分割して新たに生成したトラックデータファイル（２）のトラック鍵データとして、新たなトラック鍵データＴＲＫ

＿２を用いた場合でも、上記式（１５）に基づいてパーツ鍵データＰＫ＿２を生成することで、テンポラリ鍵データを分割前のテンポラリ鍵データと同じにできる。その結果、クラスタ鍵データも分割前のクラスタ鍵データＣＫ＿１と同じにでき、トラックデータファイル（２）内のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

また、同様に、分割後のトラックデータファイル（１）のパーツ鍵データＰＫ＿１’も、クラスタ鍵データＣＫ＿１を変えないように、トラック鍵データＴＲＫ＿１’に応じた決定される。その結果、分割後のトラックデータファイル（１）内のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要もない。

そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。

【０１１２】

次に、トラックデータファイルの結合編集処理について説明する。

図２２は、携帯用プレーヤ４の編集モジュール４４によるトラックデータファイルの結合編集処理を説明するための図である。

図２２に示すように、編集モジュール４４は、例えば、図２２（Ａ）に示すトラックデータファイル（１）と、図２２（Ｂ）に示すトラックデータファイル（２）とを結合して、図２２（Ｃ）に示すトラックデータファイル（３）を生成する。

【０１１３】

当該結合により、結合前のトラックデータファイル（１）からなるパーツ（１）と、結合前のトラックデータファイル（２）からなるパーツ（２）とを含む新たなトラックデータファイル（３）が生成される。

また、トラックデータファイル（３）のトラック鍵データとして新たなトラック鍵データＴＲＫ＿３が生成され、パーツ（１）のパーツ鍵データＰＫ＿３＿１およびパーツ（２）のパーツ鍵データＰＫ＿３＿２が後述するようにして新たに生成される。

また、トラック管理ファイル１００に、当該トラックデータファイル（３）に

対応する図６に示すＴＲＫＩＮＦおよびＰＲＴＩＮＦが追加され、当該ＴＲＫＩＮＦおよびＰＲＴＩＮＦにに、新たに生成された鍵データが後述するように設定される。

また、パーツ（１）の図６に示すＰＲＴＳＩＺＥが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル（１）のクラスタＣＬ（０）およびＣＬ（４）がそれぞれ設定される。また、パーツ（２）のＰＲＴＳＩＺＥが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル（２）のクラスタＣＬ（０）およびＣＬ（５）がそれぞれ設定される。

【０１１４】

図２３は、携帯用プレーヤ４の編集モジュール４４において、新たに生成したトラックデータファイル（３）のパーツ（１）および（２）のパーツ鍵データを生成する処理を説明するための図である。

なお、本実施形態では、結合の対象となるトラックデータファイル（１）がトラック鍵データＴＲＫ＿１、パーツ鍵データＰＫ＿１およびクラスタ鍵データＣＫ＿１を用いており、トラックデータファイル（２）がトラック鍵データＴＲＫ＿２、パーツ鍵データＰＫ＿２およびクラスタ鍵データＣＫ＿２を用いてる場合を例示して説明する。

【０１１５】

ここで、トラックデータファイル（３）は新たなトラック鍵データＴＲＫ＿３を得るが、パーツ（１）および（２）のパーツ鍵データを以下に示すように算出することで、各クラスタのクラスタ鍵データＣＫ＿１およびＣＫ＿２を結合前と同じにできる。

【０１１６】

ステップＳ１００：編集モジュール４４は、トラックデータファイルの結合指示を入力したか否かを判断し、入力したと判断した場合にはステップＳ１０１の処理を実行し、入力していないと判断した場合にはステップＳ１００の処理を繰り返す。

【０１１７】

ステップＳ１０１：編集モジュール４４は、乱数発生ユニット６０に乱数を発

生させ、当該乱数に応じたトラック鍵データＴＲＫ＿３を新たに生成する。

【０１１８】

ステップＳ１０２：編集モジュール４４は、トラックデータファイル（３）のパーツ（１）のパーツ鍵データＰＫ＿３＿１を下記式（１６）に基づいて生成する。

【０１１９】

【数１６】

$$PK\_3\_1 = TRK\_1 \ XOR \ PK\_1 \ XOR \ TRK\_3 \quad \cdots (16)$$

【０１２０】

これにより、前記式（１１）に基づいて生成されるパーツ（１）のテンポラリ鍵データを結合前のトラックデータファイル（１）のテンポラリ鍵データと同じにでき、その結果、前記式（１２）に基づいて生成されるパーツ（１）のクラスタ鍵データも結合前のトラックデータファイル（１）のクラスタ鍵データＣＫ＿１と同じにできる。

そのため、パーツ（１）のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【０１２１】

ステップＳ１０３：編集モジュール４４は、トラックデータファイル（３）のパーツ（２）のパーツ鍵データＰＫ＿３＿２を下記式（１７）に基づいて生成する。

【０１２２】

【数１７】

$$PK\_3\_2 = TRK\_2 \ XOR \ PK\_2 \ XOR \ TRK\_3 \quad \cdots (17)$$

【０１２３】

これにより、前記式（１１）に基づいて生成されるパーツ（２）のテンポラリ鍵データを結合前のトラックデータファイル（２）のテンポラリ鍵データと同じにでき、その結果、前記式（１２）に基づいて生成されるパーツ（２）のクラス

タ鍵データも結合前のトラックデータファイル（２）のクラスタ鍵データＣＫ＿２と同じにできる。

そのため、パーツ（２）のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要がない。

【０１２４】

ステップＳ１０４：携帯用記憶装置３の暗号化／復号ユニット５４において、ステップＳ１０１で生成したトラック鍵データＴＲＫ＿３を、記憶ユニット５１に記憶されている記憶用鍵データSK_mを用いて暗号化し、当該暗号化したトラック鍵データＴＲＫ＿３をフラッシュメモリ３４内のトラックデータファイル（３）に対応する図６に示すＴＲＫＩＮＦに書き込む。

【０１２５】

ステップＳ１０５：編集モジュール４４は、ステップＳ１０２およびＳ１０３で生成したパーツ鍵データＰＫ＿３＿１およびＰＫ＿３＿２をフラッシュメモリ３４内のトラックデータファイル（３）のそれぞれパーツ（１）およびパーツ（２）に対応する図６に示すＰＲＴＩＮＦにそのまま書き込む。

【０１２６】

このように、オーディオシステム１では、結合して新たに生成したトラックデータファイル（３）のトラック鍵データとして、新たなトラック鍵データＴＲＫ＿３を用いた場合でも、上記式（１６）および（１７）に基づいてパーツ鍵データＰＫ＿３＿１およびＰＫ＿３＿２を生成することで、各パーツのテンポラリ鍵データを結合前と同じにできる。その結果、各パーツのクラスタ鍵データも結合前のクラスタ鍵データＣＫ＿１およびＣＫ＿２とそれぞれ同じにでき、パーツ（１）および（２）内のサウンドユニットＳＵを新たなクラスタ鍵データを用いて再度暗号化する必要がない。そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。

【０１２７】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ＡＴＲＡＣ３方式の圧縮の単位であるサウンドユニットＳＵのバイト数（１６０バイト）が、ＣＢＣモードの暗号化の単位で

ある暗号化ブロックのバイト数（８バイト）の整数倍になる場合を例示したが、本発明は、例えば、整数倍にならない場合には、サウンドユニットＳＵにデータ長調整用のデータであるパディング(padding) を挿入して調整するようにしてもよい。

【０１２８】

また、上述した実施形態では、携帯用記憶装置３と携帯用プレーヤ４との間で相互認証処理を行う場合に、図１４に示すように、先ず始めに携帯用記憶装置３で生成した乱数R_{ms}を携帯用プレーヤ４に出力する場合を例示したが、先ず始めに携帯用プレーヤ４で生成した乱数を携帯用記憶装置３に出力するようにしてもよい。

【０１２９】

また、上述した実施形態では、図１３に示すように、記憶ユニット５１および６１に３２組の認証鍵データおよびマスター鍵データを記憶した場合を例示したが、これらの組の数は２以上であれば任意である。

【０１３０】

また、上述した実施形態では、図１３に示すように、携帯用プレーヤ４において、マスター鍵データMK_0 ～MK_{31}から認証鍵データIK_0 ～IK_{31}を生成する場合を例示したが、携帯用プレーヤ４に、携帯用記憶装置３と同じように、認証鍵データIK_0 ～IK_{31}を記憶し、乱数R_j に応じた認証鍵データを選択するようにしてもよい。

【０１３１】

また、上述した実施形態では、図１３に示すように、携帯用記憶装置３および携帯用プレーヤ４において、携帯用プレーヤ４で生成した乱数R_j を用いて、認証鍵データIK_j およびマスター鍵データMK_j を選択する場合を例示したが、携帯用記憶装置３で生成した乱数を用いてもよいし、携帯用記憶装置３および携帯用プレーヤ４の双方で発生した乱数を用いてもよい。

【０１３２】

また、上述した実施形態では、図１３に示すように、携帯用記憶装置３および携帯用プレーヤ４において乱数R_j に基づいて認証鍵データIK_j およびマスタ

ー鍵データMK_jを選択する場合を例示したが、本発明は、例えば、携帯用記憶装置３および携帯用プレーヤ４に外部から５ビットの鍵選択指示データを入力し、当該鍵選択指示データで指示される相互に対応する認証鍵データIK_jおよびマスター鍵データMK_jを、携帯用記憶装置３および携帯用プレーヤ４で選択してもよい。

【０１３３】

また、上述した実施形態では、トラックデータとしてオーディオデータを含むデータを例示したが、本発明は、その他、動画像データ、静止画像データ、文書データおよびプログラムデータなどを含むトラックデータをフラッシュメモリ３４に記憶する場合にも適用できる。

【０１３４】

【発明の効果】

以上説明したように、本発明のデータ処理装置、データ処理システムおよびその方法によれば、記憶手段に記憶された暗号化されたデータを、所定の処理ブロックを単位として効率的に処理できる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のオーディオシステムのシステム構成図である。

【図２】

図２は、図１に示す携帯用記憶装置および携帯用プレーヤの内部構成図である。

【図３】

図３は、図２に示す携帯用記憶装置内の記憶ユニットに記憶されているデータを説明するための図である。

【図４】

図４は、図２に示す携帯用記憶装置のフラッシュメモリに記憶されるデータを説明するための図である。

【図５】

図５は、図４に示すトラック管理ファイルのフォーマットを説明するための図

である。

【図６】

図６は、図５に示すＴＲＫＩＮＦおよびＰＲＴＩＮＦの詳細なフォーマットを説明するための図である。

【図７】

図７は、図４に示すトラックデータファイルの構成を説明するための図である。

【図８】

図８は、図７に示すクラスタＣＬの構成を説明するための図である。

【図９】

図９は、図２に示す携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための図である。

【図１０】

図１０は、図２に示す携帯用プレーヤの暗号化／復号ユニットのＣＢＣモードにおける暗号化処理を説明するための図である。

【図１１】

図１１は、図２に示す携帯用プレーヤの暗号化／復号ユニットのＣＢＣモードにおける復号処理を説明するための図である。

【図１２】

図１２は、図２に示す携帯用プレーヤから携帯用記憶装置への書き込み動作を説明するためのフローチャートである。

【図１３】

図１３は、図２に示す相互認証ユニットによる認証鍵データIK_jの選択処理を説明するための図である。

【図１４】

図１４は、図２に示す携帯用記憶装置と携帯用プレーヤとの間の相互認証処理を説明するための図である。

【図１５】

図１５は、セッション鍵データＳｅｋの生成処理を説明するための図である。

【図１６】

図１６は、図２に示す携帯用プレーヤから携帯用記憶装置へのオーディオデータの書き込み処理を説明するための図である。

【図１７】

図１７は、図２に示す携帯用記憶装置から携帯用プレーヤへの読み出し動作を説明するためのフローチャートである。

【図１８】

図１８は、図２に示す携帯用記憶装置から携帯用プレーヤへのオーディオデータの読み出し処理を説明するための図である。

【図１９】

図１９は、携帯用プレーヤの編集モジュールによるトラックデータファイルの分割編集処理を説明するための図である。

【図２０】

図１９に示す分割編集処理を行った後のクラスタ内のデータを説明するための図である。

【図２１】

図２１は、図２に示す携帯用プレーヤの編集モジュールにおいて、分割編集時に、新たなトラックデータファイルのトラック鍵データおよびパーツ鍵データを生成する方法を説明するための図である。

【図２２】

図２２は、図２に示す携帯用プレーヤの編集モジュールによるトラックデータファイルの結合編集処理を説明するための図である。

【図２３】

図２３は、図２に示す携帯用プレーヤ４の編集モジュールにおいて、新たに生成したトラックデータファイル（３）のパーツ（１）および（２）のパーツ鍵データを生成する処理を説明するための図である。

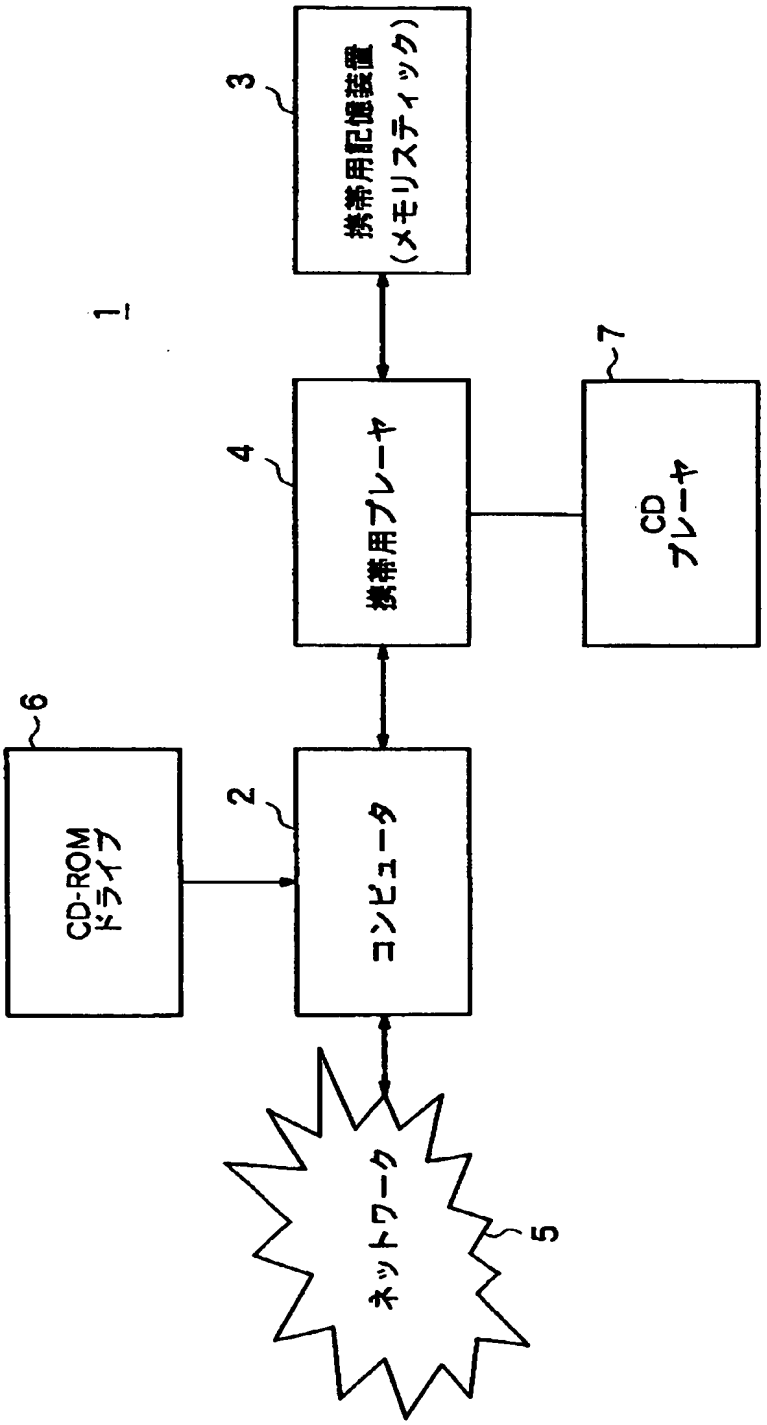
【符号の説明】

１…オーディオシステム、２…コンピュータ、３…携帯用記憶装置、４…携帯用プレーヤ、５…ネットワーク、３３，４３…制御モジュール、５０，６０…乱

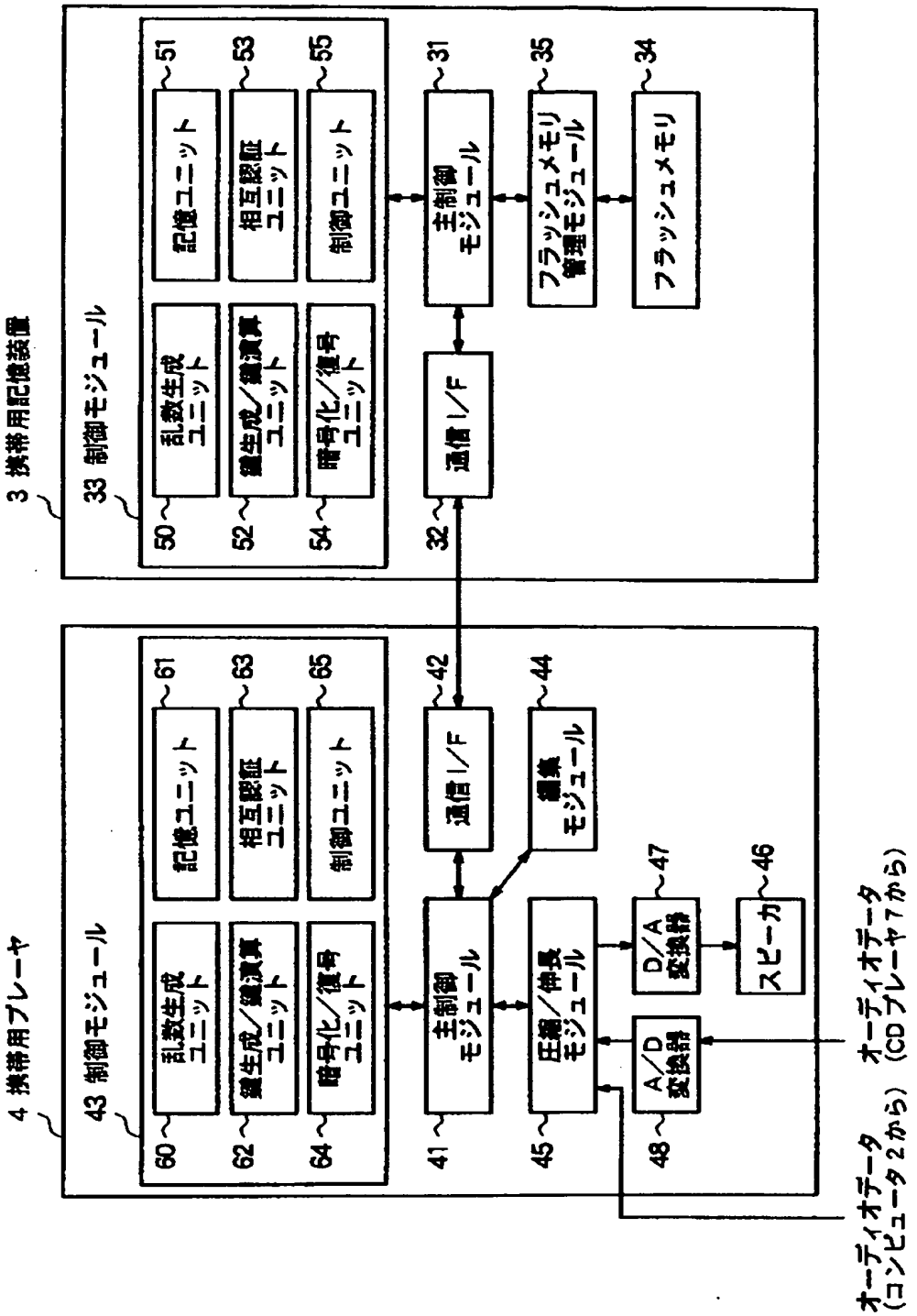
数発生ユニット、５１，６１…記憶ユニット、５２，６２…鍵生成／演算ユニット、５３，６３…相互認証ユニット、５４，７４…暗号化／復号ユニット、５５，６５…制御ユニット、３４…フラッシュメモリ、４４…編集モジュール、４５…圧縮／伸長モジュール、４６…スピーカ

【書類名】　図面

【図１】


1
2
3
4
5
6
7
携帯用記憶装置
（メモリスティック）
携帯用プレーヤ
CD
プレーヤ
コンピュータ
CD-ROM
ドライブ
ネットワーク

【図２】

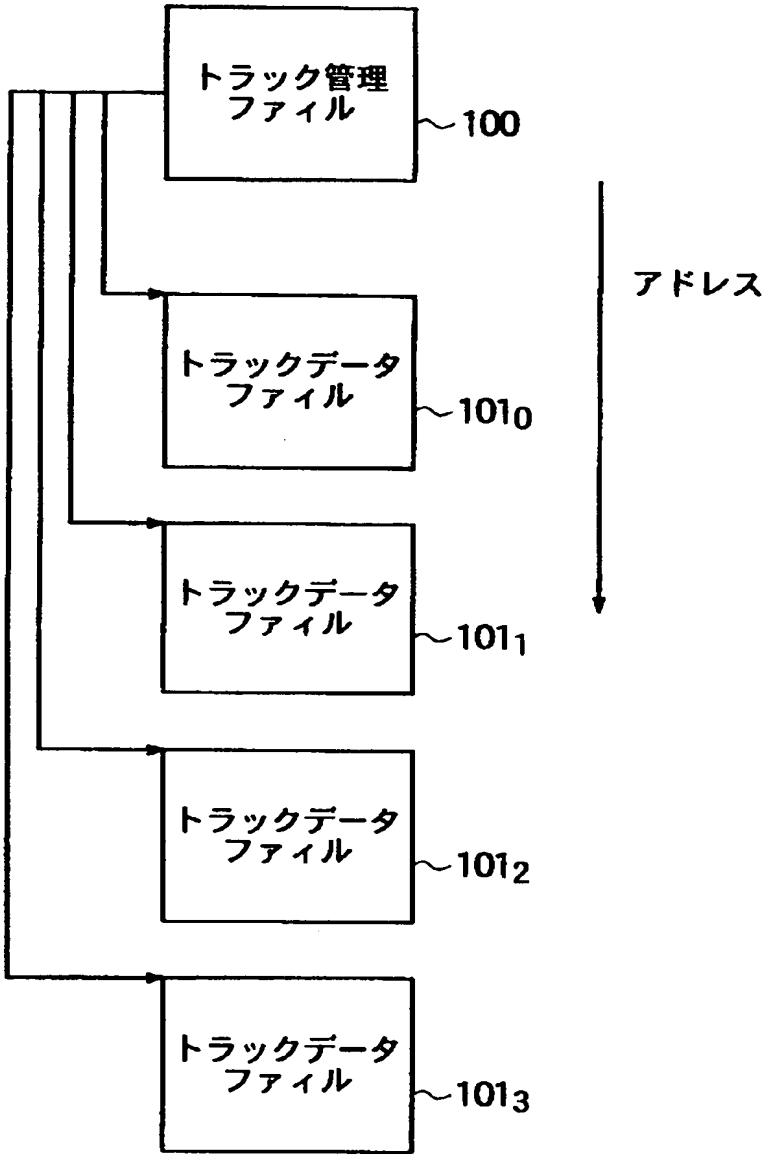

3 携帯用記憶装置
33 制御モジュール
50 乱数生成ユニット
51 記憶ユニット
52 鍵生成／鍵演算ユニット
53 相互認証ユニット
54 暗号化／復号ユニット
55 制御ユニット
32 通信I／F
31 主制御モジュール
35 フラッシュメモリ管理モジュール
34 フラッシュメモリ
4 携帯用プレーヤ
43 制御モジュール
60 乱数生成ユニット
61 記憶ユニット
62 鍵生成／鍵演算ユニット
63 相互認証ユニット
64 暗号化／復号ユニット
65 制御ユニット
41 主制御モジュール
42 通信I／F
45 圧縮／伸長モジュール
44 編集モジュール
48 A／D変換器
47 D／A変換器
46 スピーカ
オーディオデータ（CDプレーヤ7から）
オーディオデータ（コンピュータ2から）

【図３】

携帯用記憶装置３の記憶ユニット51に記憶されるデータ

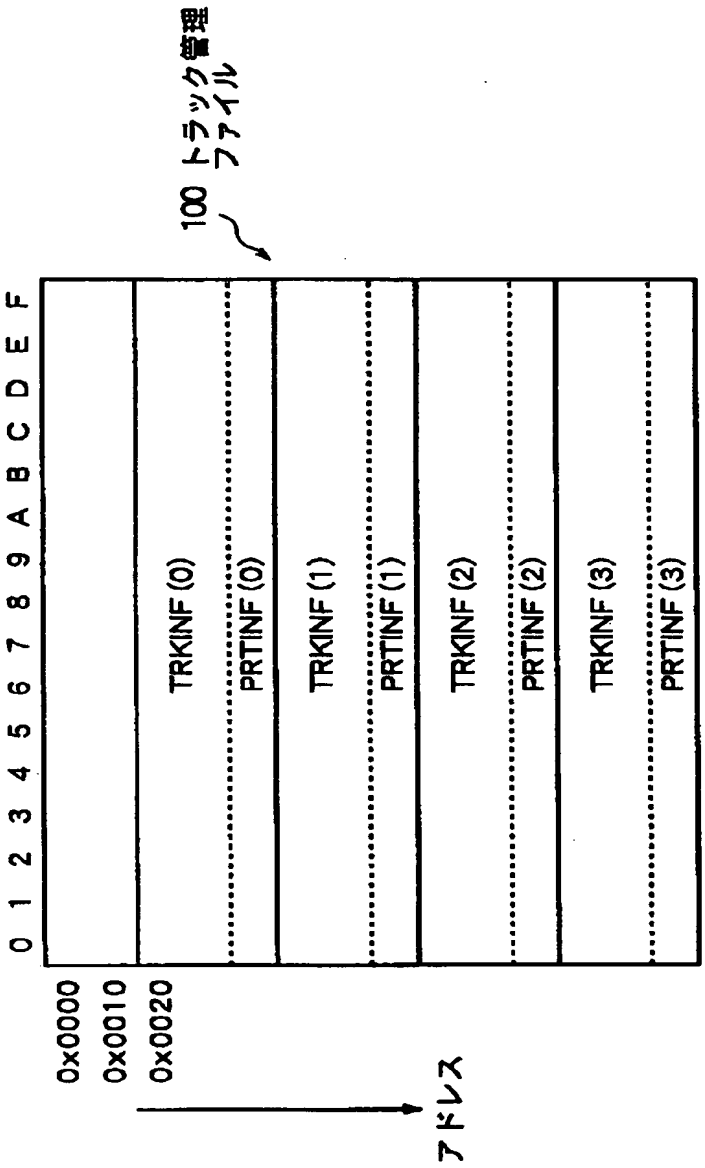
認証鍵データ	IK_0
	IK_1
	IK_2
	IK_3
	⋮
	IK_{30}
	IK_{31}
装置識別データ	ID_m
記憶用鍵データ	SK_m

【図４】

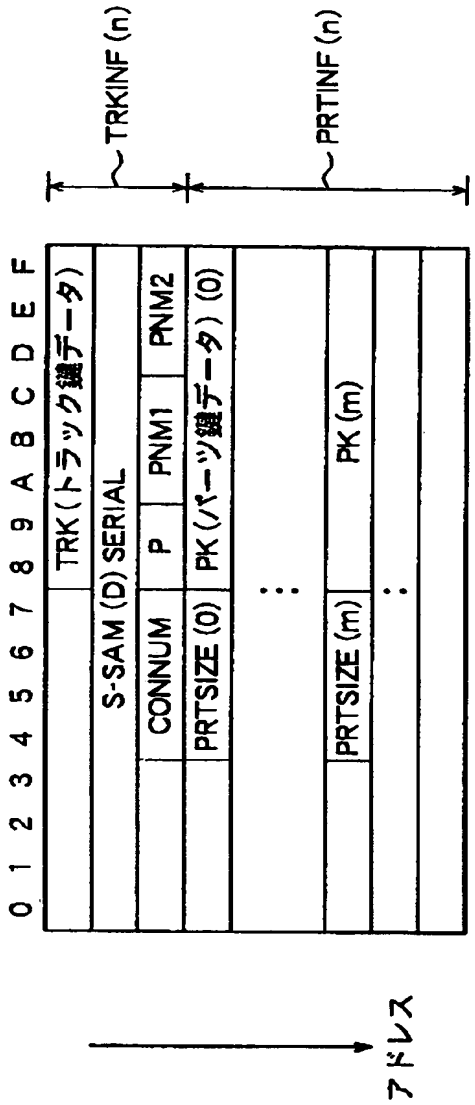


携帯用記憶装置３のフラッシュメモリ34の記憶データ

【図５】

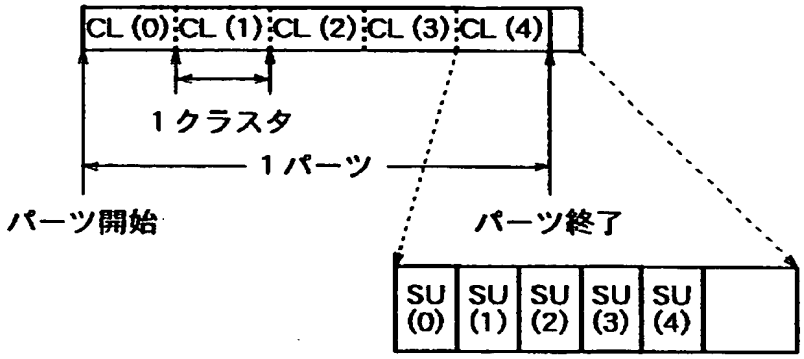

100 トラック管理ファイル
0 1 2 3 4 5 6 7 8 9 A B C D E F
TRKINF (0)
PRTINF (0)
TRKINF (1)
PRTINF (1)
TRKINF (2)
PRTINF (2)
TRKINF (3)
PRTINF (3)
0x0000
0x0010
0x0020
アドレス

【図６】

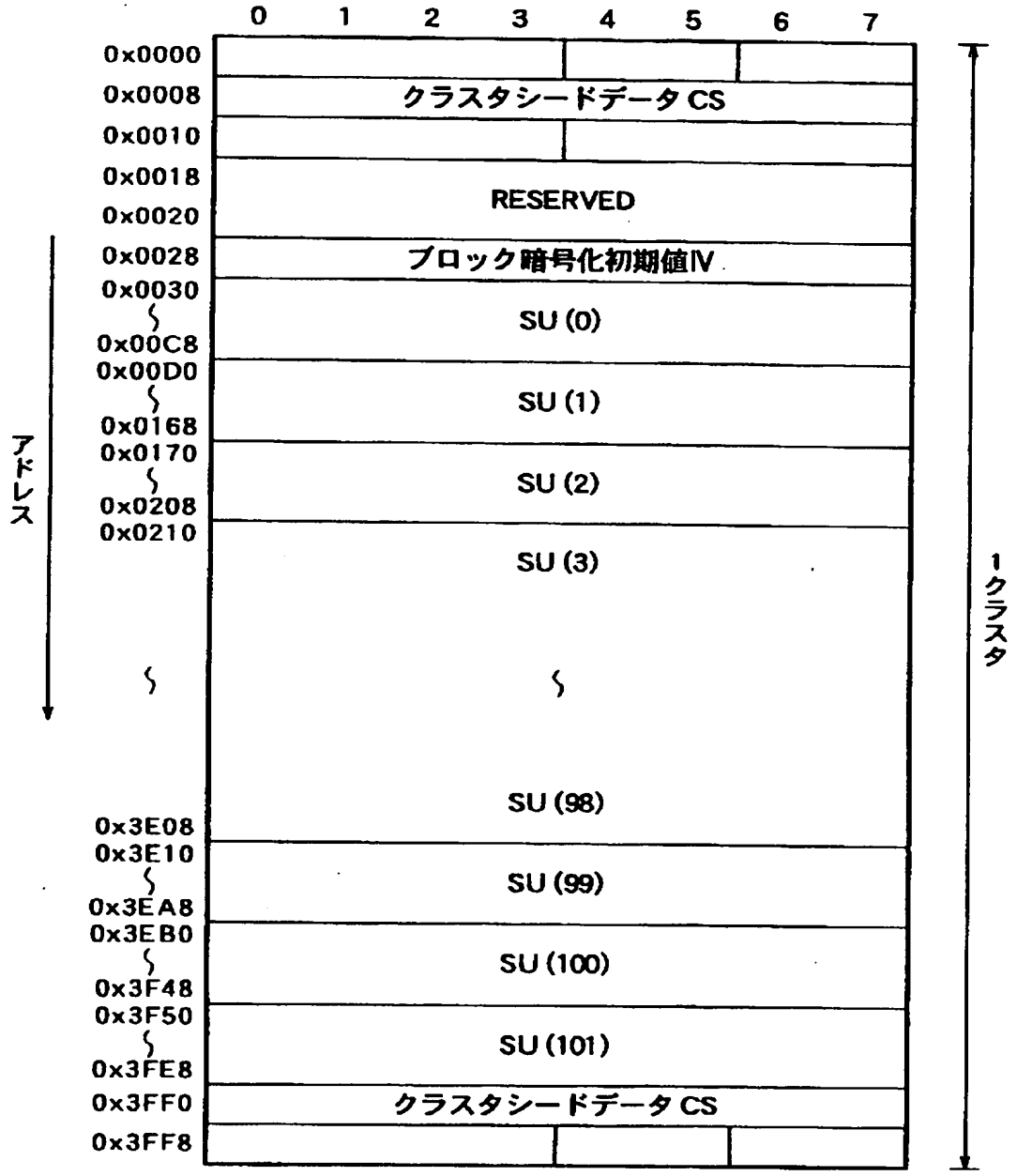

TRKINF (n)
PRTINF (n)
0 1 2 3 4 5 6 7 8 9 A B C D E F
TRK (トラック鍵データ)
S-SAM (D) SERIAL
CONNUM
P
PNM1
PNM2
PRTSIZE (0)
PK (パーツ鍵データ) (0)
PRTSIZE (m)
PK (m)
アドレス

【図７】

トラックデータファイル 101_0



【図８】


0 1 2 3 4 5 6 7
0x0000
0x0008
クラスタシードデータCS
0x0010
0x0018
0x0020
RESERVED
0x0028
ブロック暗号化初期値IV
0x0030
0x00C8
SU (0)
0x00D0
0x0168
SU (1)
0x0170
0x0208
SU (2)
0x0210
SU (3)
SU (98)
0x3E08
0x3E10
0x3EA8
SU (99)
0x3EB0
0x3F48
SU (100)
0x3F50
0x3FE8
SU (101)
0x3FF0
クラスタシードデータCS
0x3FF8
アドレス
1クラスタ

【図９】

携帯用プレーヤ４の記憶モジュール41に記憶されるデータ

マスター鍵データ MK_0

MK_1

MK_2

MK_3

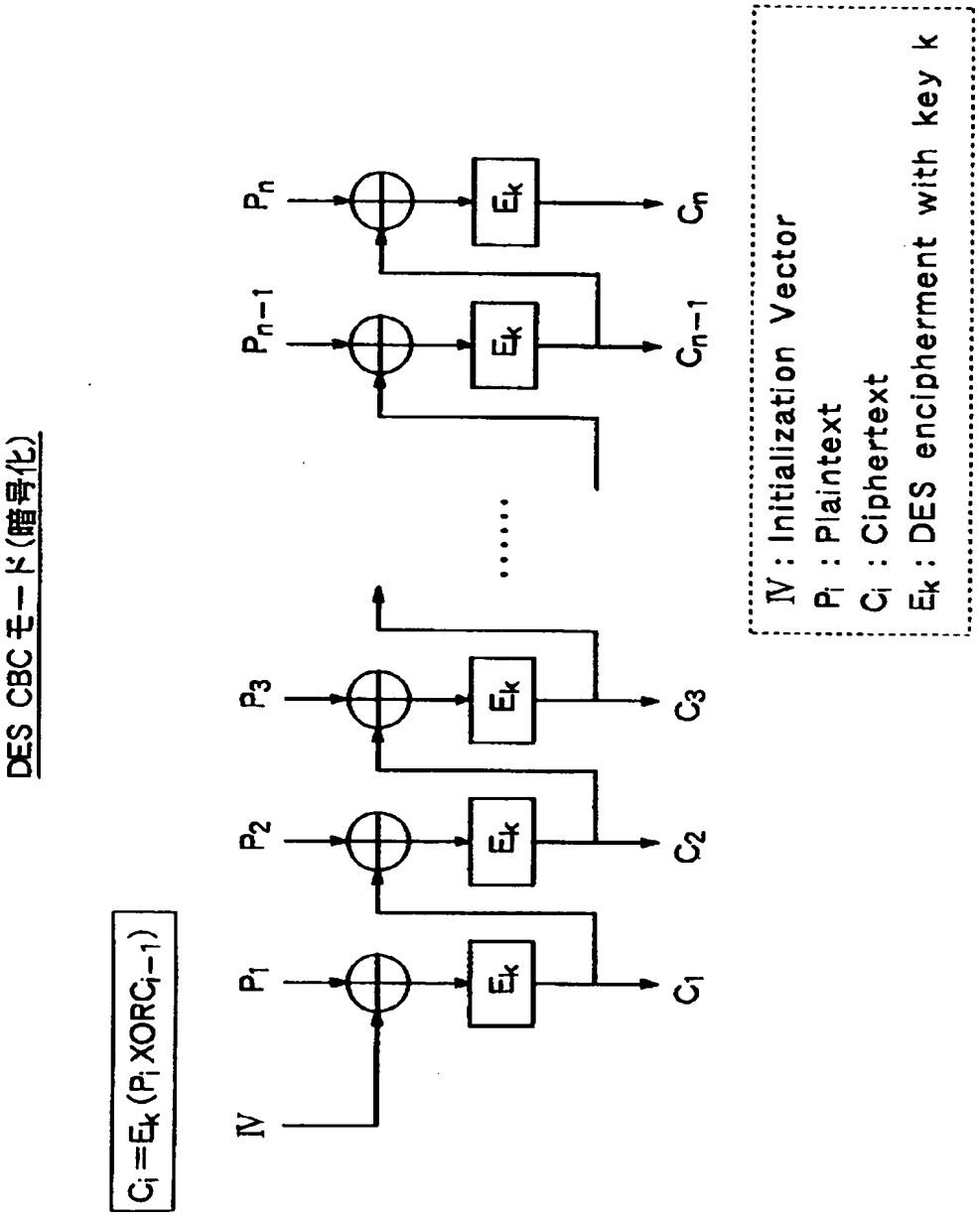
⋮

MK_{30}

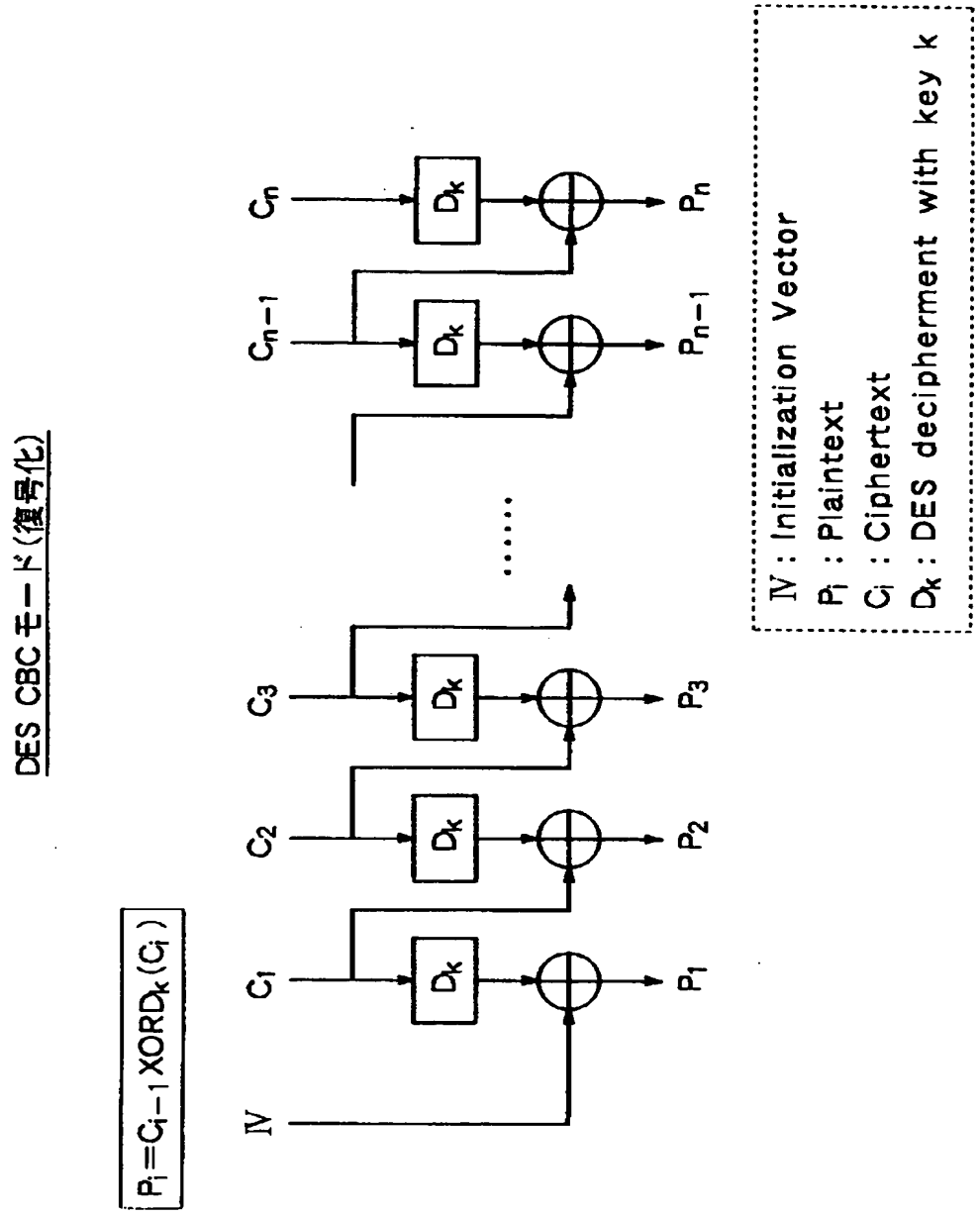
MK_{31}

装置識別データ ID_d

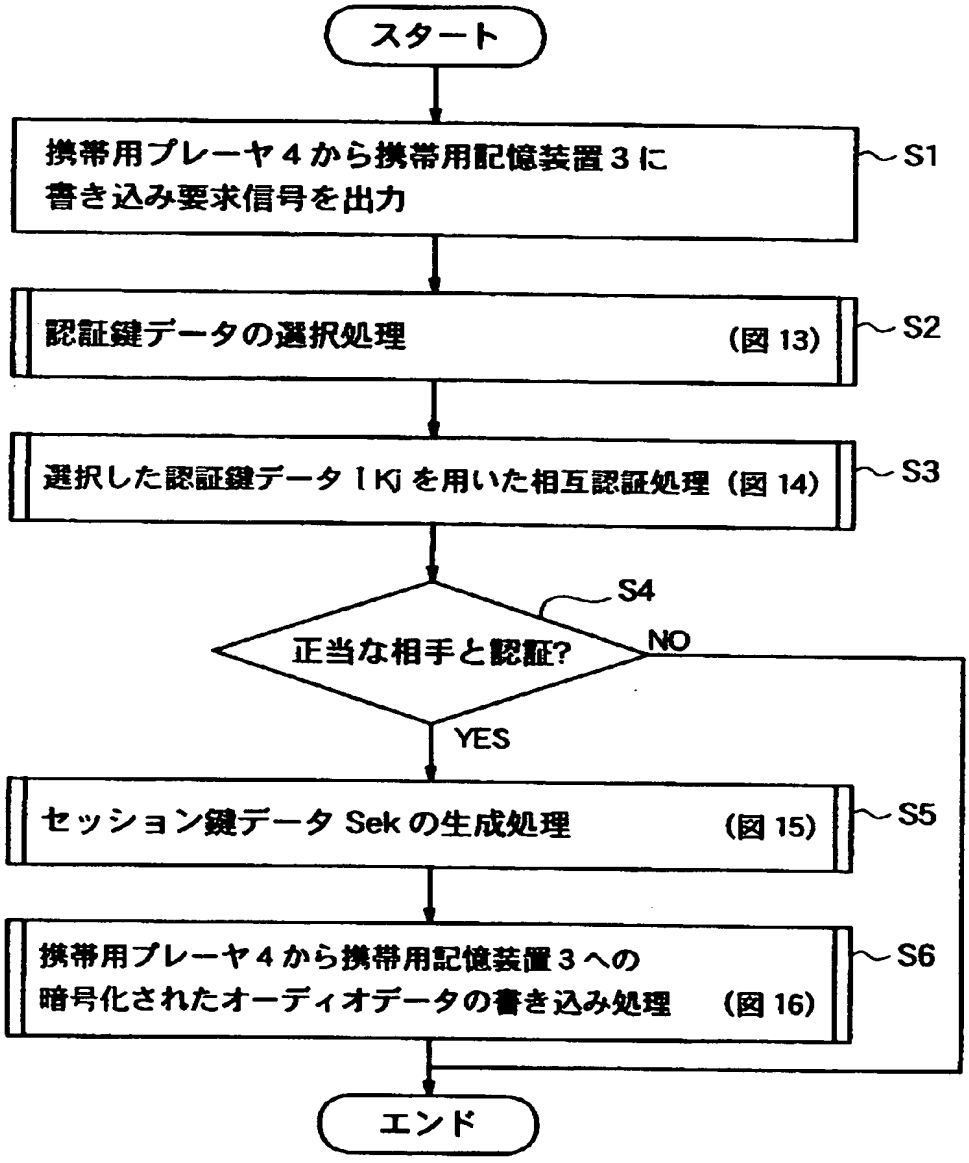
【図１０】


DES CBC モード(暗号化)
$C_i = E_k(P_i \text{ XOR } C_{i-1})$
IV
P_1
P_2
P_3
P_{n-1}
P_n
E_k
C_1
C_2
C_3
C_{n-1}
C_n
IV : Initialization Vector
P_i : Plaintext
C_i : Ciphertext
E_k : DES encipherment with key k

【図１１】

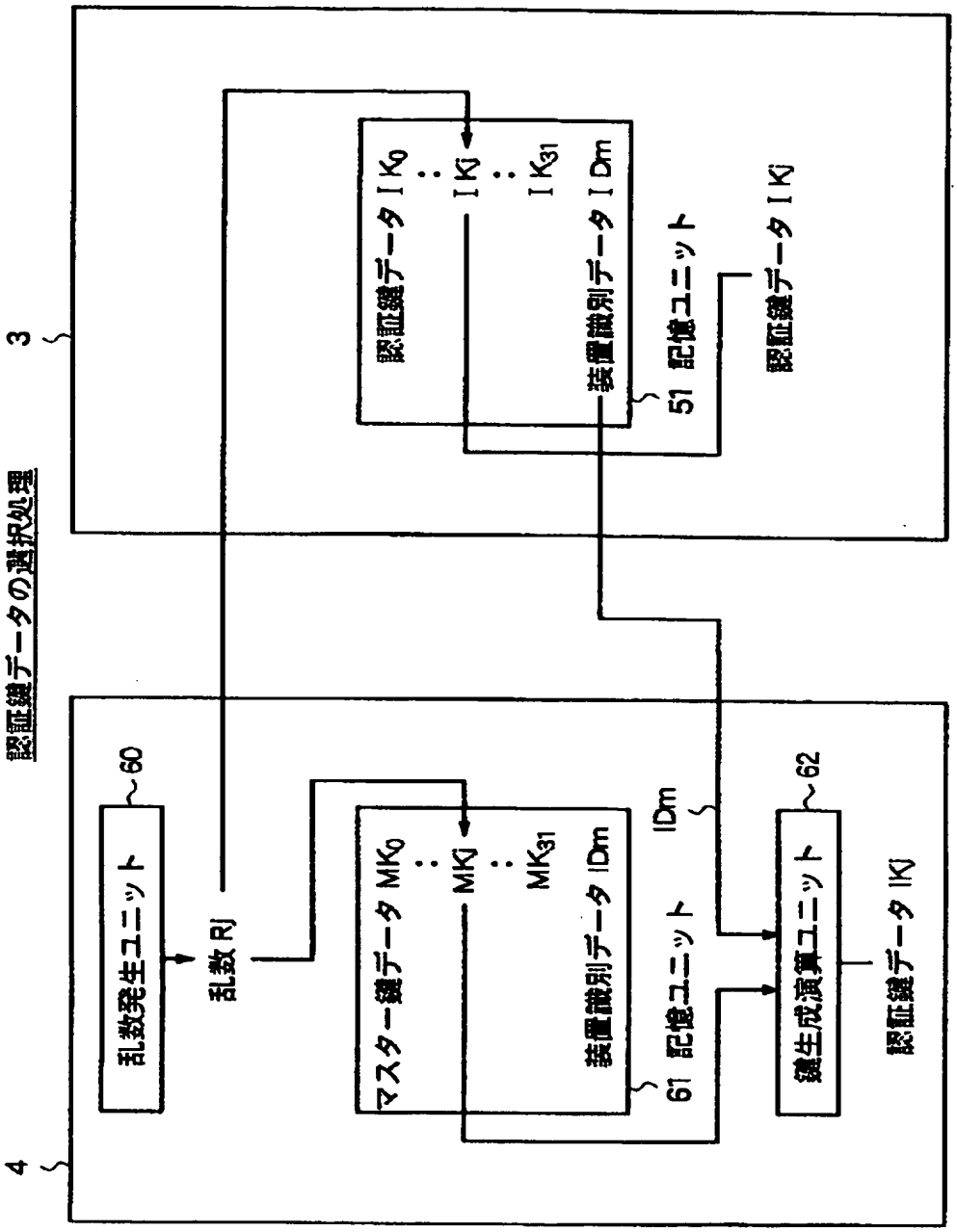

DES CBC モード(復号化)
$P_i=C_{i-1}$ XOR$D_k(C_i)$
IV
C_1
C_2
C_3
C_{n-1}
C_n
D_k
P_1
P_2
P_3
P_{n-1}
P_n
IV : Initialization Vector
P_i : Plaintext
C_i : Ciphertext
D_k : DES decipherment with key k

【図１２】

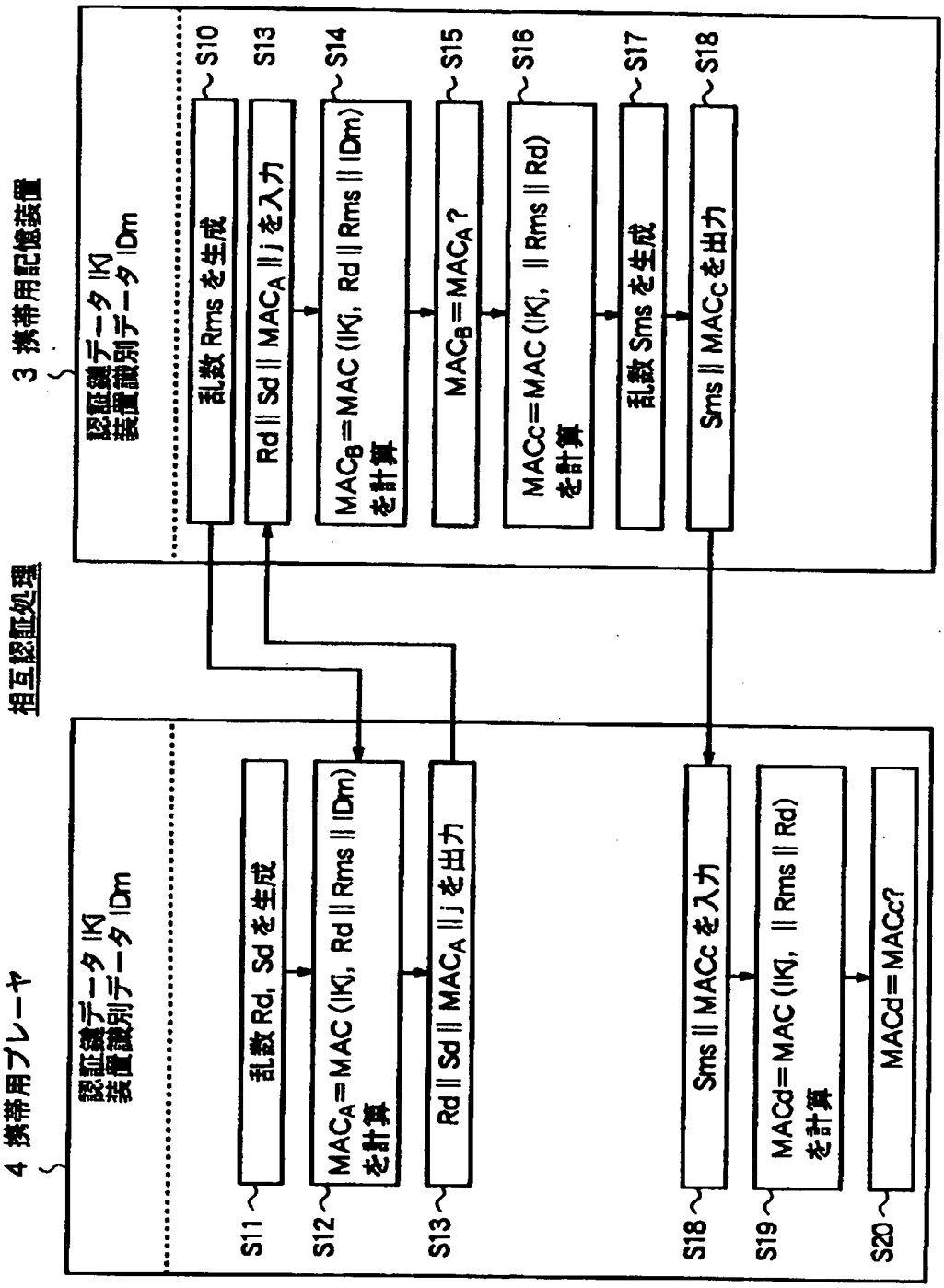


携帯用記憶装置３への書込処理

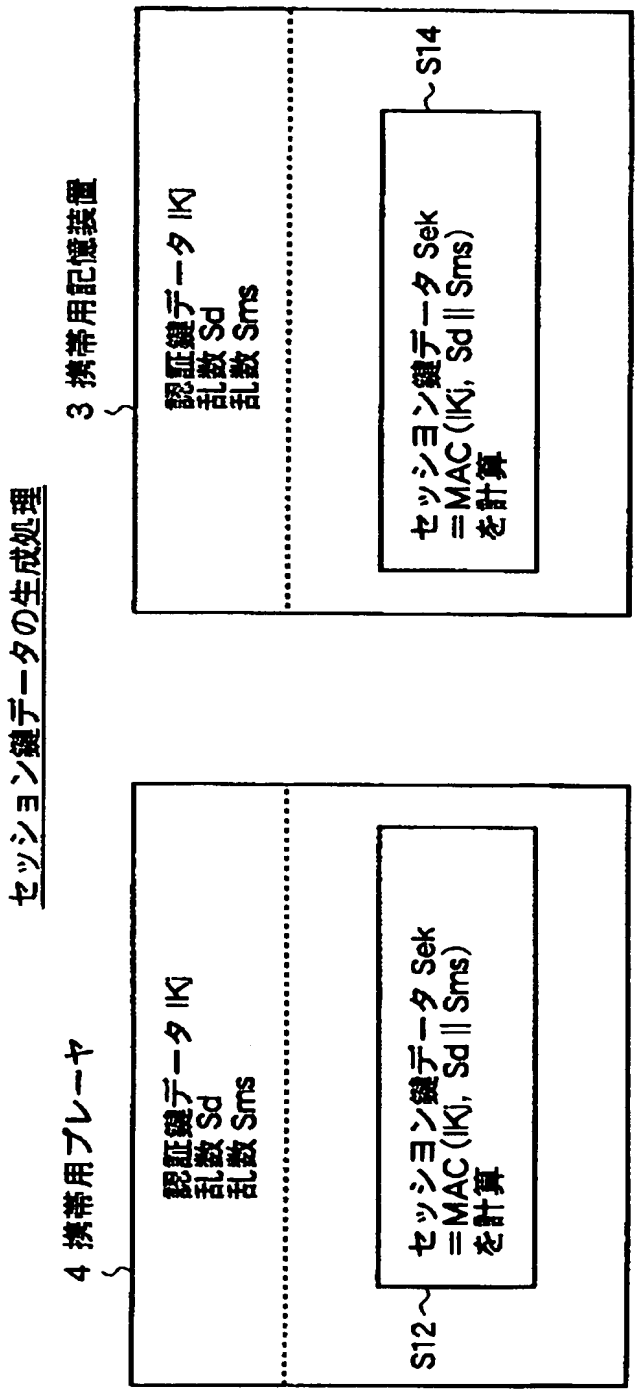
【図１３】


認証鍵データの選択処理
3
4
認証鍵データ IK0
IKj
IK31
装置識別データ IDm
51 記憶ユニット
認証鍵データ IKj
乱数発生ユニット
60
乱数 RJ
マスター鍵データ MK0
MKj
MK31
装置識別データ IDm
61 記憶ユニット
IDm
62
鍵生成演算ユニット
認証鍵データ IKj

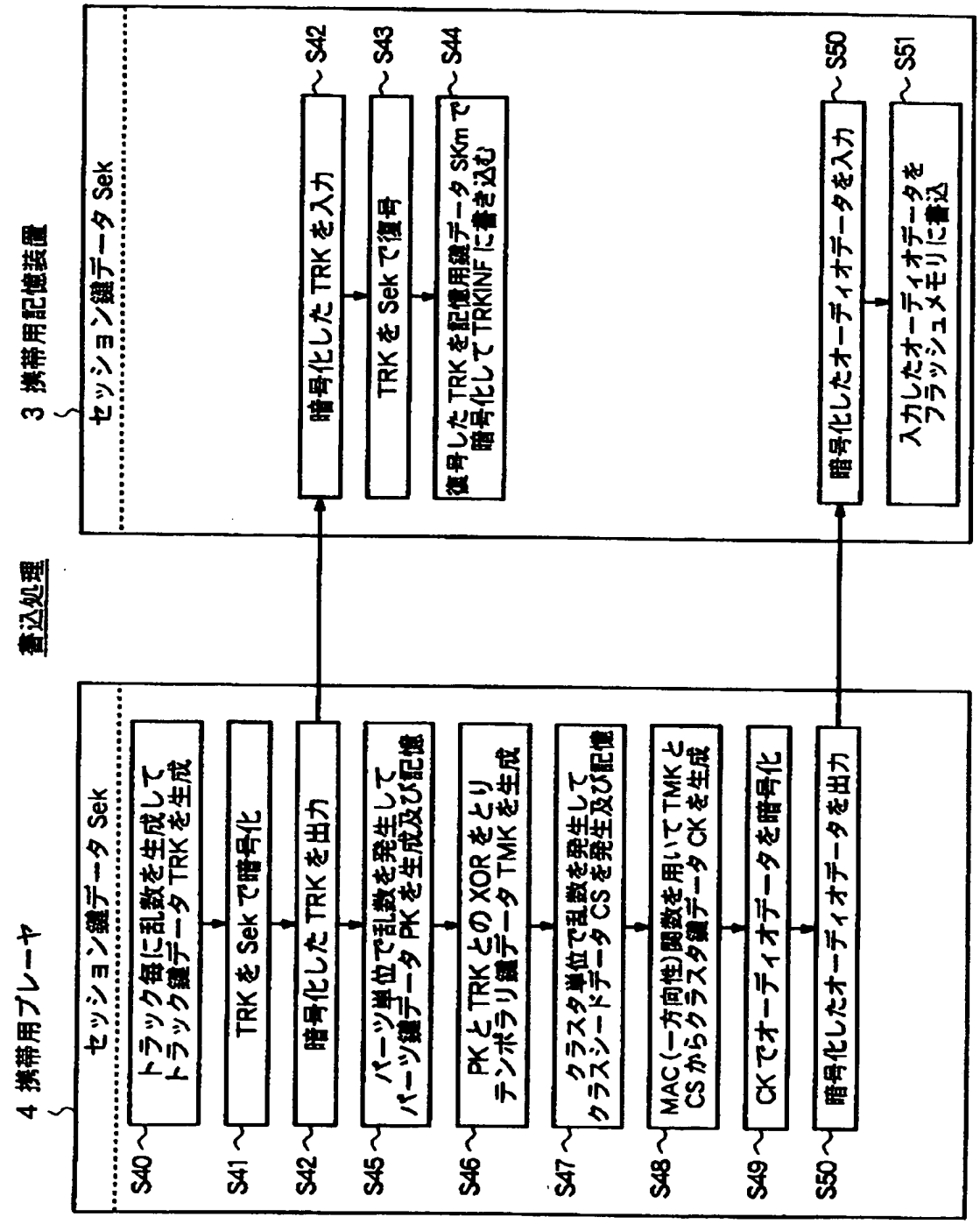
【図１４】


3 携帯用記憶装置
認証鍵データ IKj
装置識別データ IDm
S10
乱数 Rms を生成
S13
Rd || Sd || MACA || j を入力
S14
MACB = MAC (IKj, Rd || Rms || IDm) を計算
S15
MACB = MACA ?
S16
MACc = MAC (IKj, || Rms || Rd) を計算
S17
乱数 Sms を生成
S18
Sms || MACc を出力
相互認証処理
4 携帯用プレーヤ
認証鍵データ IKj
装置識別データ IDm
S11
乱数 Rd, Sd を生成
S12
MACA = MAC (IKj, Rd || Rms || IDm) を計算
S13
Rd || Sd || MACA || j を出力
S18
Sms || MACc を入力
S19
MACd = MAC (IKj, || Rms || Rd) を計算
S20
MACd = MACc?

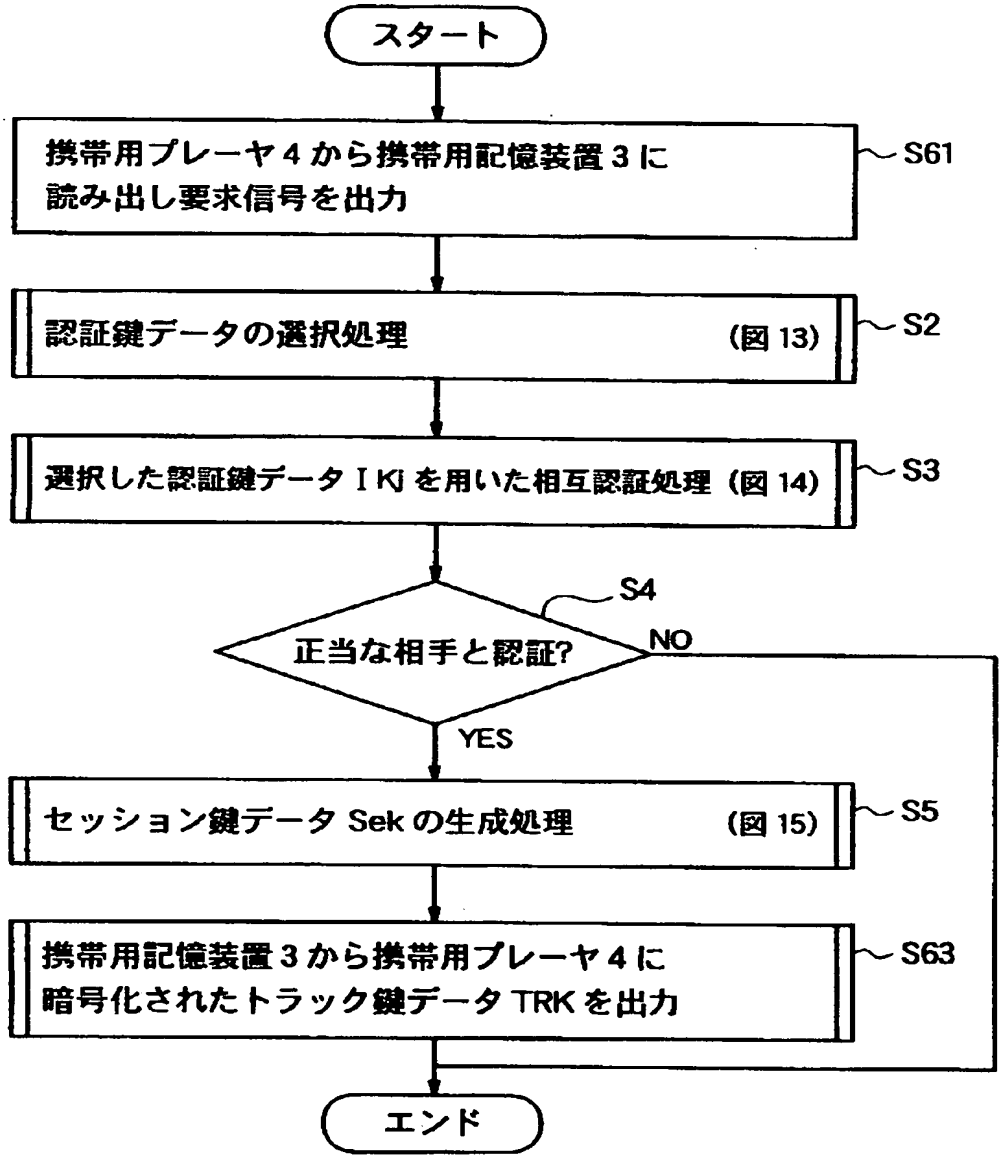
【図１５】


セッション鍵データの生成処理
3 携帯用記憶装置
認証鍵データ IKj
乱数 Sd
乱数 Sms
S14
セッション鍵データ Sek
=MAC(IKj, Sd || Sms)
を計算
4 携帯用プレーヤ
認証鍵データ IKj
乱数 Sd
乱数 Sms
S12
セッション鍵データ Sek
=MAC(IKj, Sd || Sms)
を計算

【図１６】

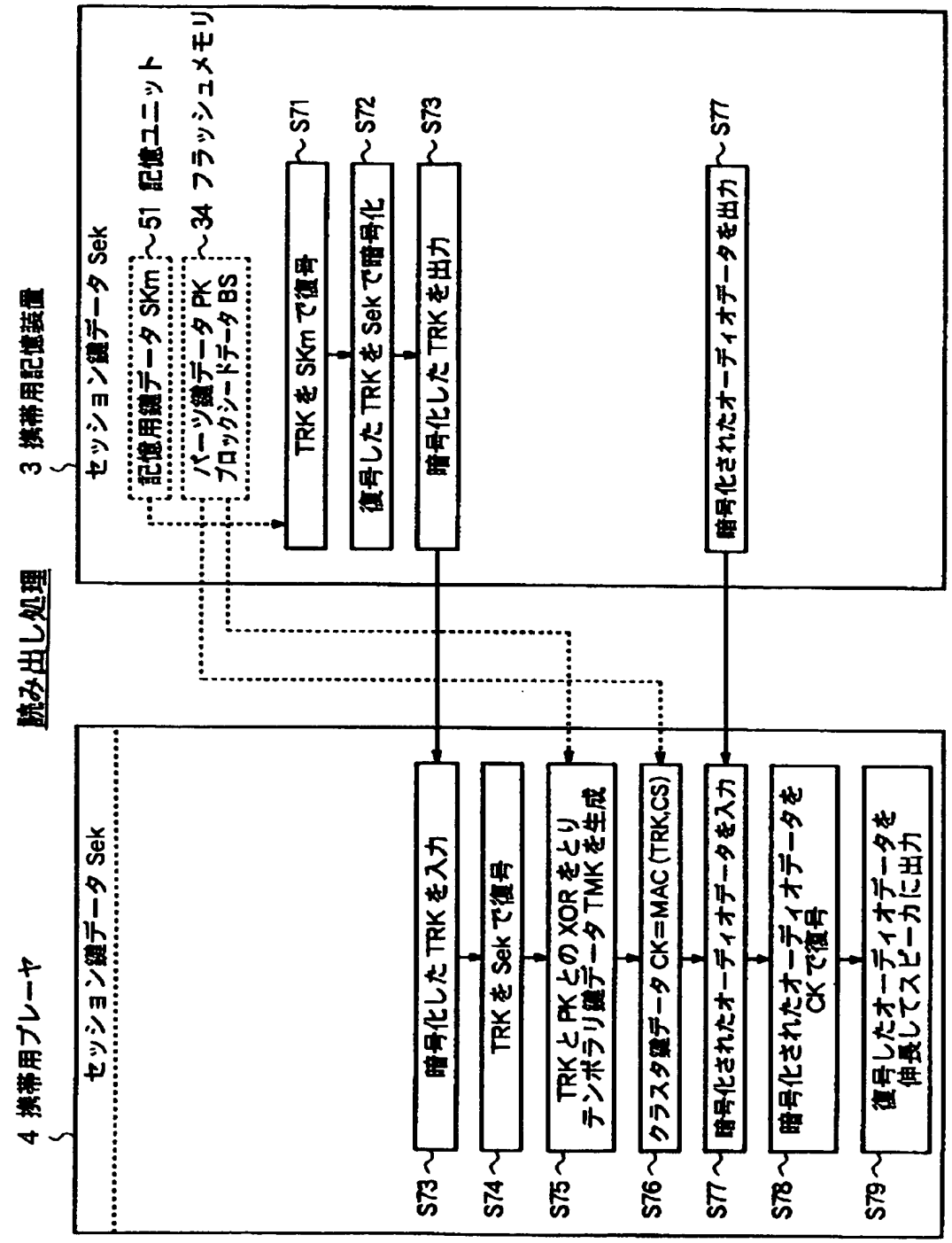

4 携帯用プレーヤ
書込処理
3 携帯用記憶装置
セッション鍵データ Sek
トラック毎に乱数を生成して
トラック鍵データ TRK を生成
TRK を Sek で暗号化
暗号化した TRK を出力
パーツ単位で乱数を発生して
パーツ鍵データ PK を生成及び記憶
PK と TRK との XOR をとり
テンポラリ鍵データ TMK を生成
クラスタ単位で乱数を発生して
クラスシードデータ CS を発生及び記憶
MAC(一方向性)関数を用いて TMK と
CS からクラスタ鍵データ CK を生成
CK でオーディオデータを暗号化
暗号化したオーディオデータを出力
暗号化した TRK を入力
TRK を Sek で復号
復号した TRK を記憶用鍵データ SKm で
暗号化して TRKINF に書き込む
暗号化したオーディオデータを入力
入力したオーディオデータを
フラッシュメモリに書込
S40
S41
S42
S45
S46
S47
S48
S49
S50
S42
S43
S44
S50
S51

【図１７】

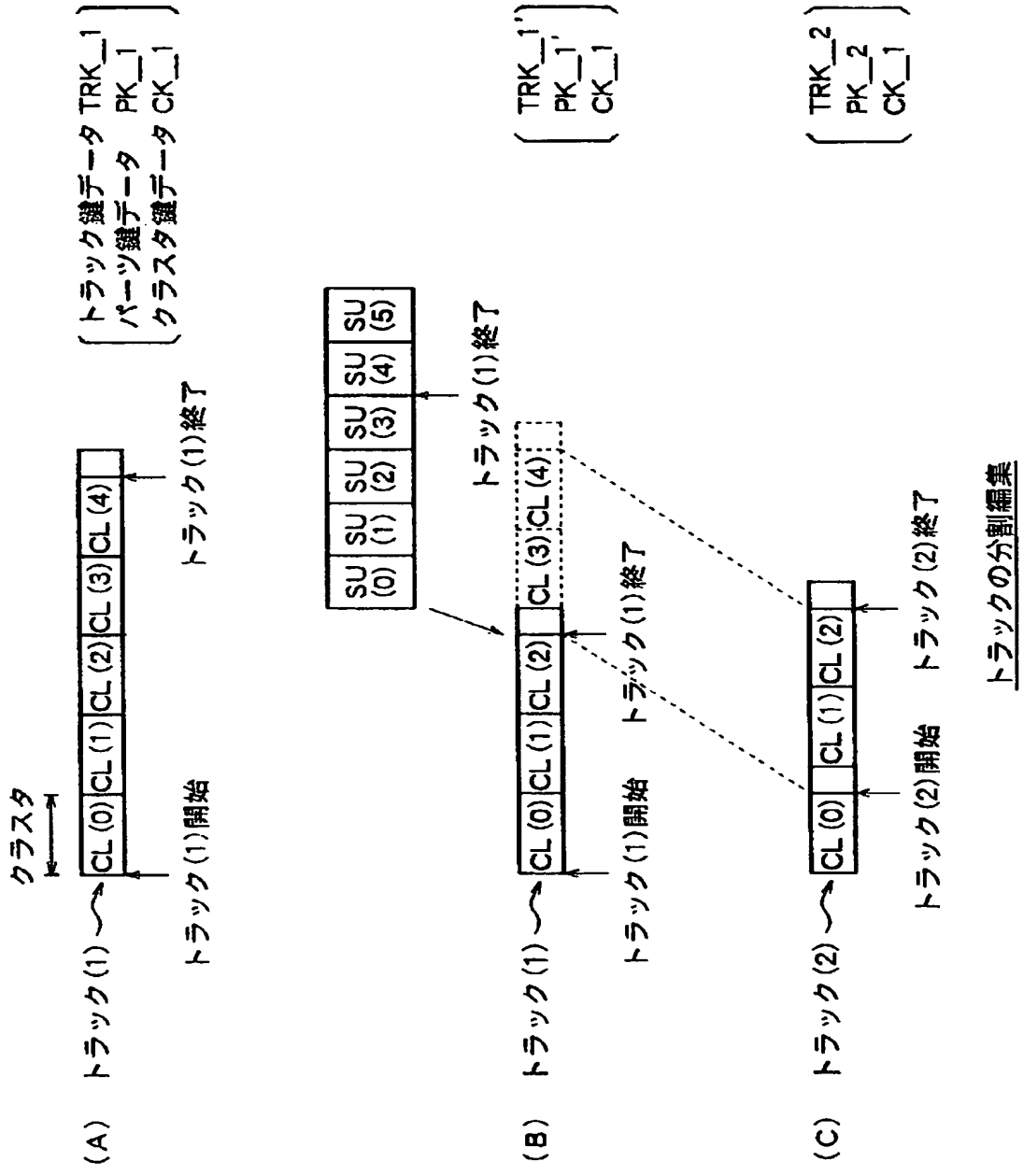


携帯用記憶装置３からの読み出し処理

【図１８】

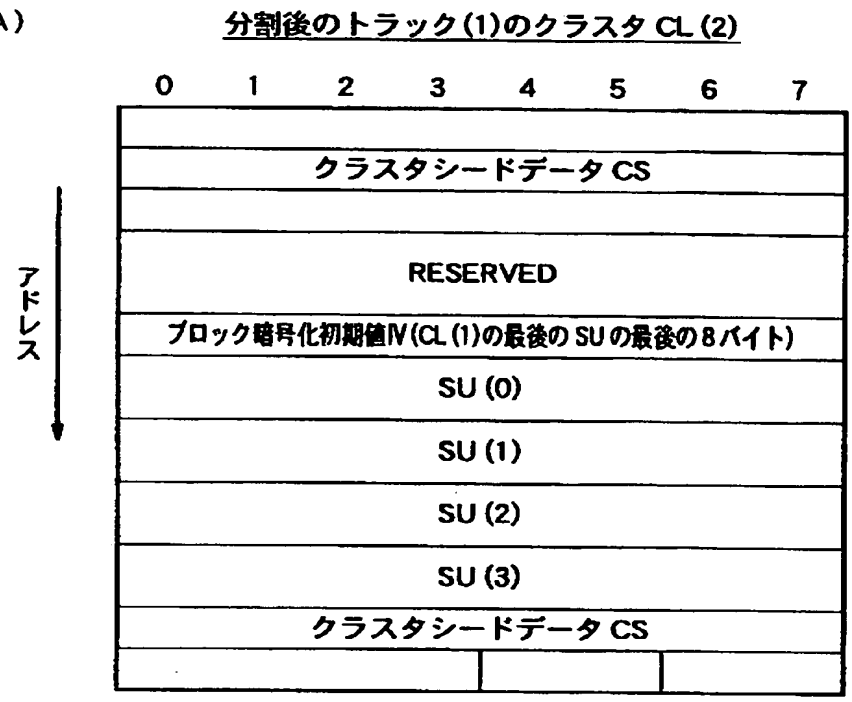

読み出し処理
3 携帯用記憶装置
セッション鍵データ Sek
記憶用鍵データ SKm
51 記憶ユニット
パーツ鍵データ PK
ブロックシードデータ BS
34 フラッシュメモリ
S71
TRK を SKm で復号
S72
復号した TRK を Sek で暗号化
S73
暗号化した TRK を出力
S77
暗号化されたオーディオデータを出力
4 携帯用プレーヤ
セッション鍵データ Sek
S73
暗号化した TRK を入力
S74
TRK を Sek で復号
S75
TRK と PK との XOR をとり テンポラリ鍵データ TMK を生成
S76
クラスタ鍵データ CK=MAC (TRK,CS)
S77
暗号化されたオーディオデータを入力
S78
暗号化されたオーディオデータを CK で復号
S79
復号したオーディオデータを 伸長してスピーカに出力

【図１９】

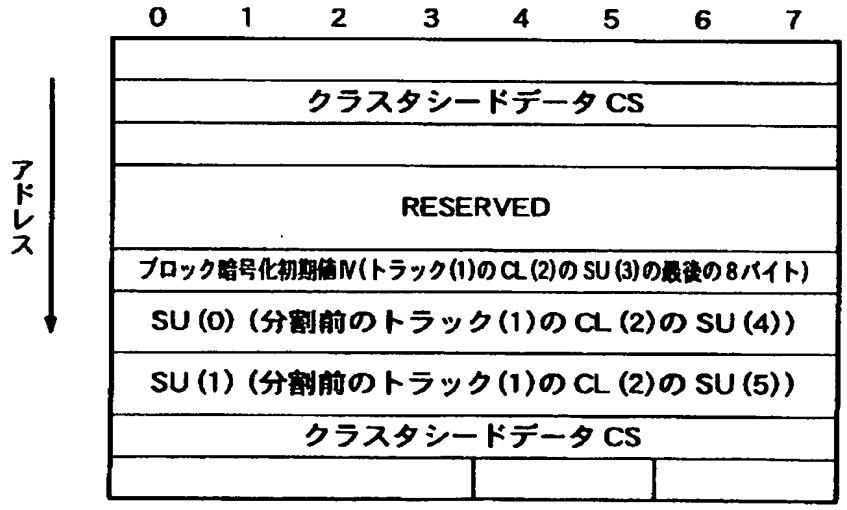

トラック鍵データ TRK_1
パージ鍵データ PK_1
クラスタ鍵データ CK_1
クラスタ
(A) トラック(1)
CL (0) CL (1) CL (2) CL (3) CL (4)
トラック(1)開始
トラック(1)終了
SU (0) SU (1) SU (2) SU (3) SU (4) SU (5)
(B) トラック(1)
CL (0) CL (1) CL (2) CL (3) CL (4)
トラック(1)開始
トラック(1)終了
TRK_1'
PK_1'
CK_1
(C) トラック(2)
CL (0) CL (1) CL (2)
トラック(2)開始
トラック(2)終了
TRK_2
PK_2
CK_1
トラックの分割編集

【図２０】

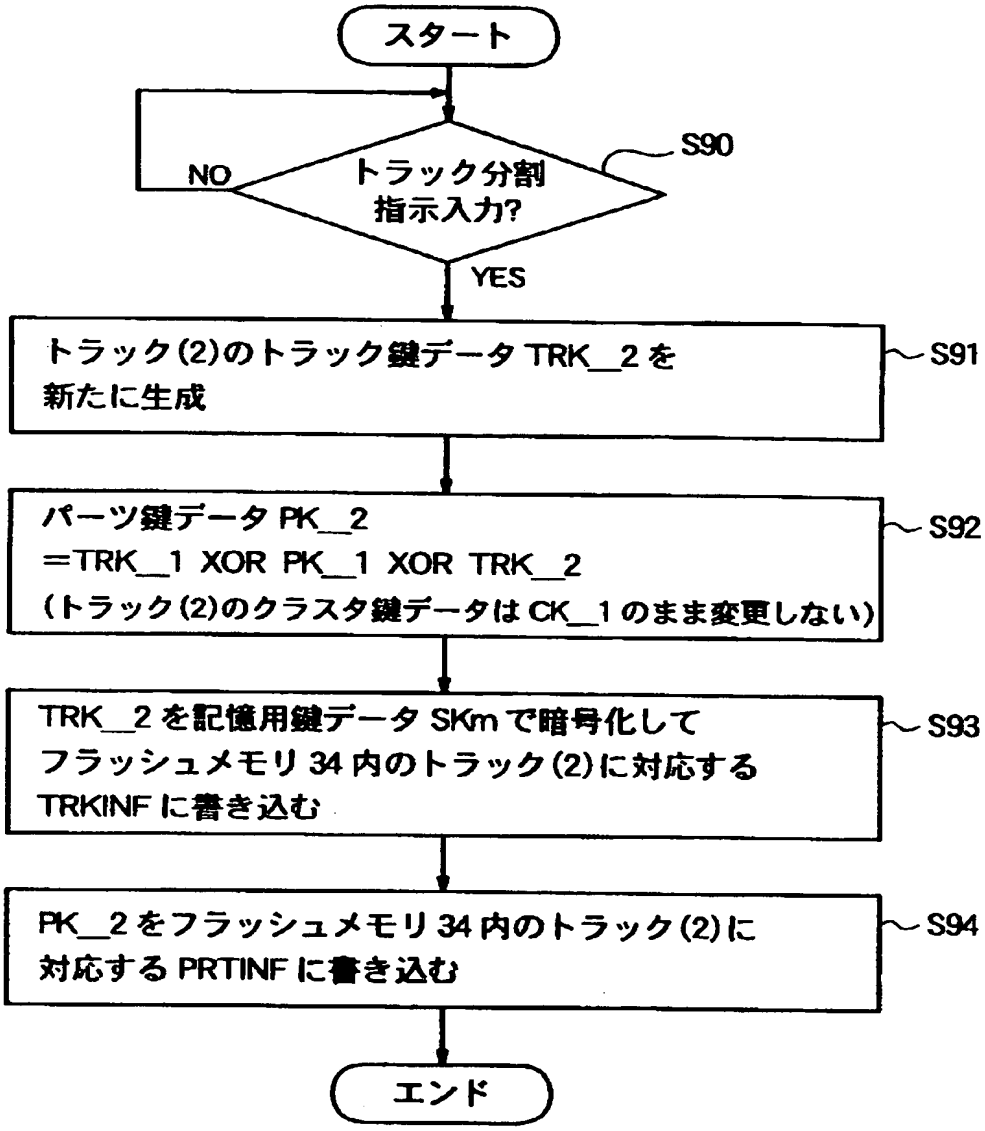
(A)


分割後のトラック(1)のクラスタ CL(2)
0 1 2 3 4 5 6 7
クラスタシードデータ CS
RESERVED
ブロック暗号化初期値IV(CL(1)の最後の SU の最後の 8 バイト)
SU (0)
SU (1)
SU (2)
SU (3)
クラスタシードデータ CS
アドレス

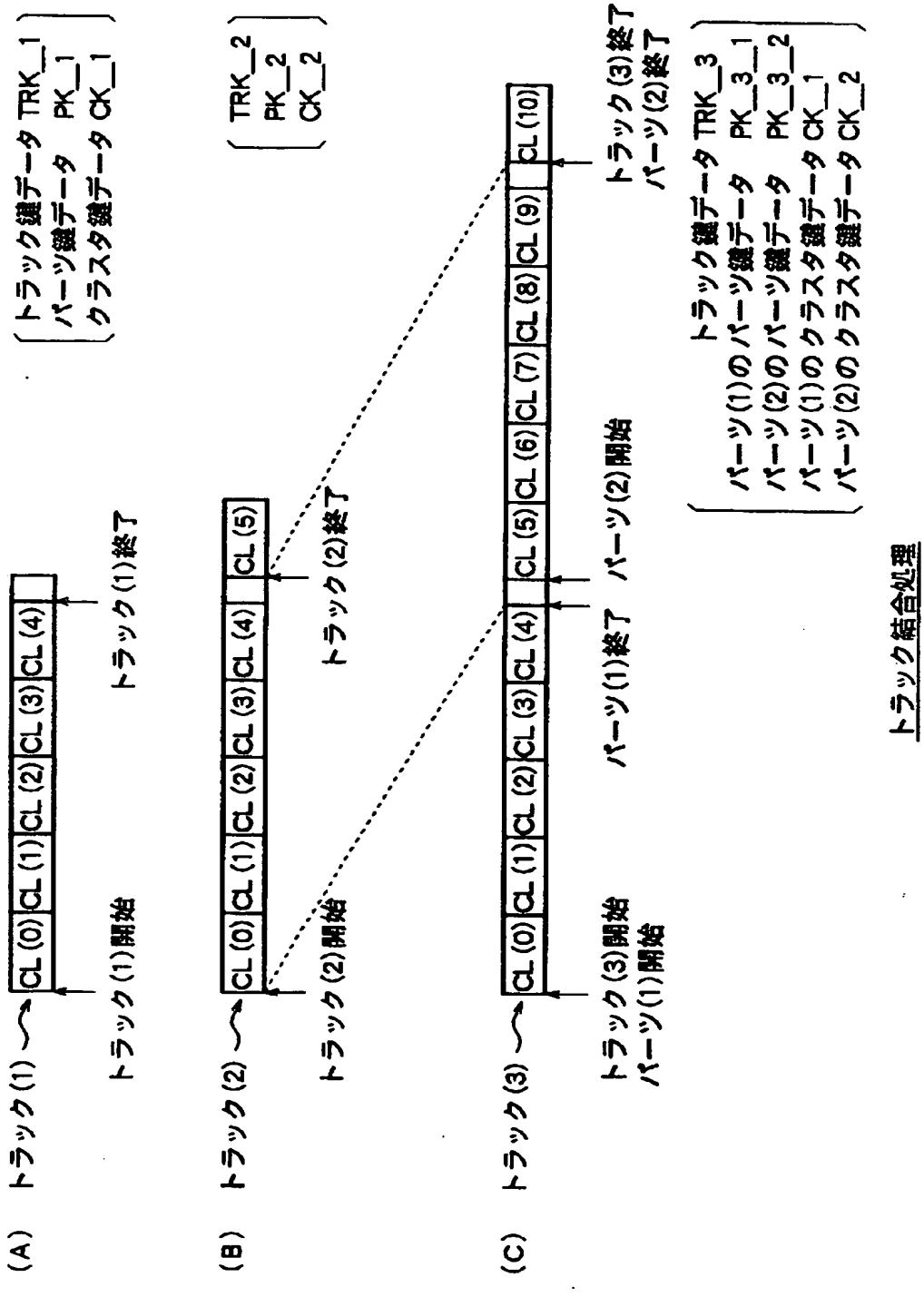
(B)


トラック(2)のクラスタ CL(0)
0 1 2 3 4 5 6 7
クラスタシードデータ CS
RESERVED
ブロック暗号化初期値IV(トラック(1)の CL(2)の SU(3)の最後の 8 バイト)
SU (0) (分割前のトラック(1)の CL (2)の SU (4))
SU (1) (分割前のトラック(1)の CL (2)の SU (5))
クラスタシードデータ CS
アドレス

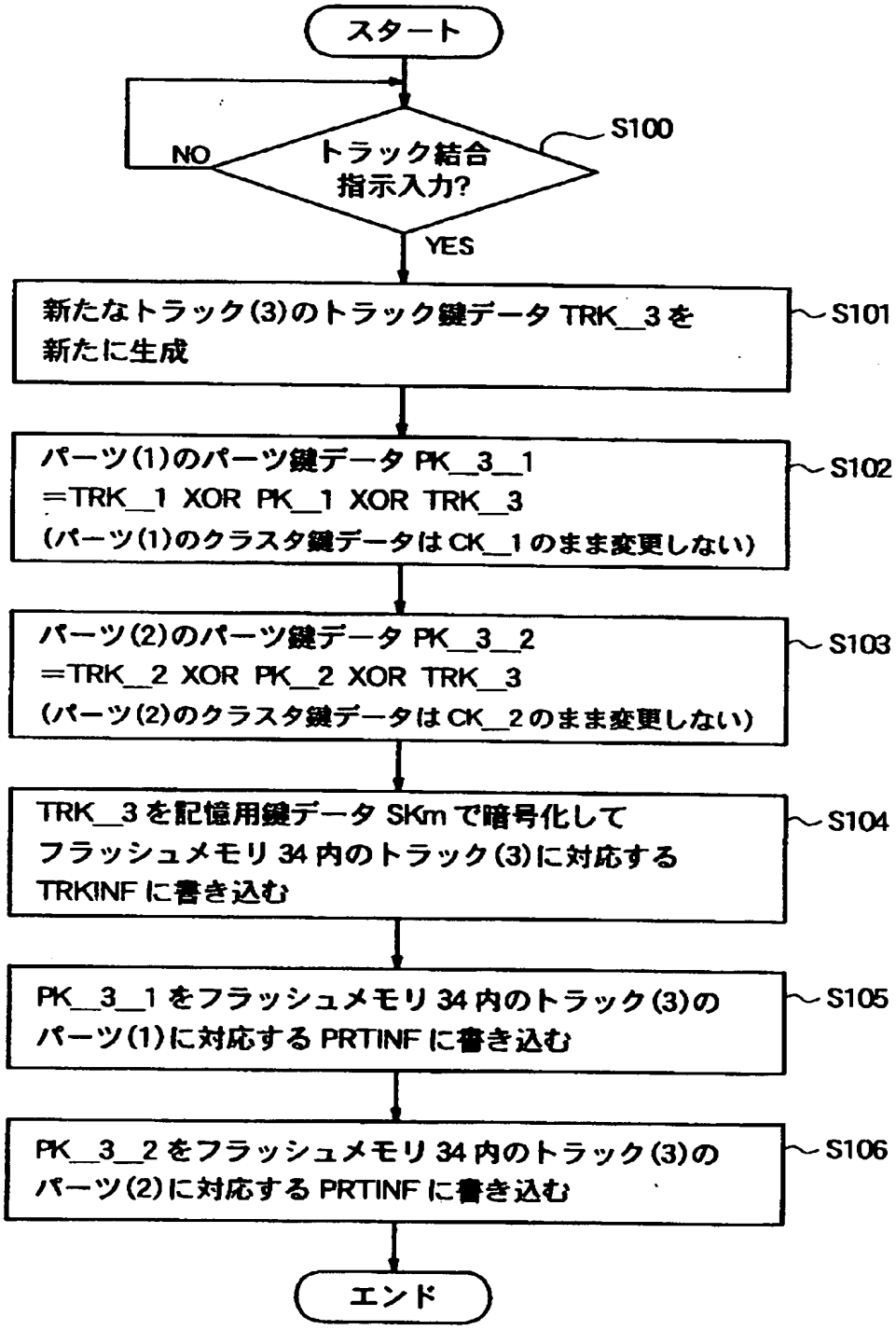
【図２１】


スタート
S90
NO
トラック分割
指示入力?
YES
トラック(2)のトラック鍵データ TRK__2 を
新たに生成
S91
パーツ鍵データ PK__2
＝TRK__1 XOR PK__1 XOR TRK__2
(トラック(2)のクラスタ鍵データは CK__1 のまま変更しない)
S92
TRK__2 を記憶用鍵データ SKm で暗号化して
フラッシュメモリ 34 内のトラック(2)に対応する
TRKINF に書き込む
S93
PK__2 をフラッシュメモリ 34 内のトラック(2)に
対応する PRTINF に書き込む
S94
エンド

【図２２】


(A) トラック(1)
CL(0) CL(1) CL(2) CL(3) CL(4)
トラック(1)開始
トラック(1)終了
トラック鍵データ TRK_1
パーツ鍵データ PK_1
クラスタ鍵データ CK_1
(B) トラック(2)
CL(0) CL(1) CL(2) CL(3) CL(4) CL(5)
トラック(2)開始
トラック(2)終了
TRK_2
PK_2
CK_2
(C) トラック(3)
CL(0) CL(1) CL(2) CL(3) CL(4) CL(5) CL(6) CL(7) CL(8) CL(9) CL(10)
トラック(3)開始
パーツ(1)開始
パーツ(1)終了
パーツ(2)開始
トラック(3)終了
パーツ(2)終了
トラック鍵データ TRK_3
パーツ(1)のパーツ鍵データ PK_3_1
パーツ(2)のパーツ鍵データ PK_3_2
パーツ(1)のクラスタ鍵データ CK_1
パーツ(2)のクラスタ鍵データ CK_2
トラック結合処理

【図２３】


スタート
S100
NO
トラック結合
指示入力?
YES
新たなトラック(3)のトラック鍵データ TRK__3 を
新たに生成
S101
パーツ(1)のパーツ鍵データ PK__3__1
=TRK__1 XOR PK__1 XOR TRK__3
(パーツ(1)のクラスタ鍵データは CK__1 のまま変更しない)
S102
パーツ(2)のパーツ鍵データ PK__3__2
=TRK__2 XOR PK__2 XOR TRK__3
(パーツ(2)のクラスタ鍵データは CK__2 のまま変更しない)
S103
TRK__3 を記憶用鍵データ SKm で暗号化して
フラッシュメモリ 34 内のトラック(3)に対応する
TRKINF に書き込む
S104
PK__3__1 をフラッシュメモリ 34 内のトラック(3)の
パーツ(1)に対応する PRTINF に書き込む
S105
PK__3__2 をフラッシュメモリ 34 内のトラック(3)の
パーツ(2)に対応する PRTINF に書き込む
S106
エンド

【書類名】　　要約書

【要約】

【課題】　例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理ブロックに基づいた処理と復号処理とを簡単な構成で正確に行うことができるデータ処理装置を提供する。

【解決手段】　所定のデータ長の暗号化ブロックを単位としてデータを暗号化／復号ユニット６４と、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う圧縮／伸長モジュール４５と、暗号化したデータを記憶するフラッシュメモリ３４とを有し、携帯用プレーヤ４は、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように前記暗号化したデータをフラッシュメモリ３４に書き込み、前記処理ブロックを単位として前記データをフラッシュメモリ３４から読み出す。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社